OPEN ACCESS

KING'S College LONDON

King's Research Portal

DOI:
10.1016/j.tcs.2017.01.027

Document Version
Peer reviewed version

Link to publication record in King's Research Portal

Citation for published version (APA):
Ayala-Rincón, M., Fernández, M., & Nantes-Sobrinho, D. (2017). Intruder deduction problem for locally stable theories with normal forms and inverses. *Theoretical Computer Science*, *672*, 64-100. [TCS-D-14-00678R4]. https://doi.org/10.1016/j.tcs.2017.01.027

Citing this paper
Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

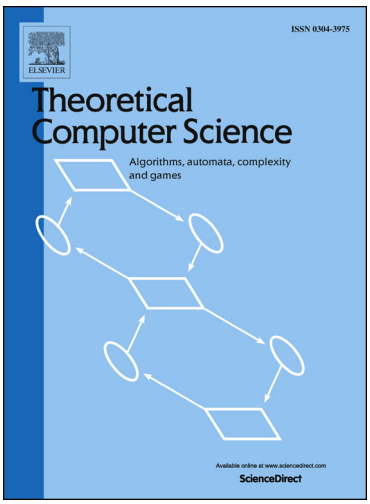
General rights
Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

•Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
•You may not further distribute the material or use it for any profit-making activity or commercial gain
•You may freely distribute the URL identifying the publication in the Research Portal

Take down policy
If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 06. May. 2023

Accepted Manuscript



Intruder deduction problem for locally stable theories with normal forms and inverses

Mauricio Ayala-Rincón, Maribel Fernández, Daniele Nantes-Sobrinho

PII: S0304-3975(17)30121-4
DOI: http://dx.doi.org/10.1016/j.tcs.2017.01.027
Reference: TCS 11066

To appear in: *Theoretical Computer Science*

Received date: 6 October 2014
Revised date: 22 December 2016
Accepted date: 12 January 2017

Please cite this article in press as: M. Ayala-Rincón et al., Intruder deduction problem for locally stable theories with normal forms and inverses, *Theoret. Comput. Sci.* (2017), http://dx.doi.org/10.1016/j.tcs.2017.01.027

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Intruder Deduction Problem for Locally Stable Theories with Normal Forms and Inverses[☆]

Mauricio Ayala-Rincón[a,b,1], Maribel Fernández[c], Daniele Nantes-Sobrinho[a,c,1,*]

[a]*Departamento de Matemática, Universidade de Brasília, Brazil.*
[b]*Departamento de Ciência da Computação, Universidade de Brasília, Brazil.*
[c]*Departament of Informatics, King's College London, Strand Campus, London, UK.*

Abstract

We present an algorithm to decide the intruder deduction problem (IDP) for a class of equational theories that include associative and commutative (AC) operators. The algorithm is based on the analysis of reductions in the head of terms built from normal contexts using the initial knowledge of the intruder. It relies on a new and efficient algorithm to solve a restricted case of higher-order AC-matching. For the subclass of theories for which *AC* operators have inverses, our algorithm runs in polynomial time on the size of a saturated set built from the initial knowledge of the intruder. To illustrate, we apply the results to Pure AC theories, Abelian Groups, Abelian Groups extended with exponentiation, and XOR. Although specific algorithms have already been defined to deal with each of these theories, we provide a modular approach that can deal with all of them in a uniform way.

Keywords: Intruder Deduction Problem, Associativity and Commutativity, Locally Stable Theories, Term Rewrite Systems, AC-matching.

1. Introduction

The *intruder deduction problem* (IDP) is the question of whether a passive eavesdropper (that is, an intruder who is passively listening to messages sent through a network) can obtain a certain information from the messages observed.

Following the approach of Dolev and Yao, we model the capabilities of an intruder by a deduction system. The IDP is formalised as the problem of deciding whether an intruder can deduce a certain information t from an initial knowledge Γ, more precisely, whether there is a proof of t from Γ. The analysis of this deduction system usually relies on the notion of a *local theory*, i.e. a theory where a simplest proof that a term t is deducible from a set Γ can consist only of subterms of Γ and t.

Inspired by the notion of *locally stable theories* introduced by Abadi and Cortier [1], in this paper we propose a method to decide the deducibility relation for subclasses of associative and

[☆]Work partially supported by grants 146/2012 CAPES-PVE, 476952/2013-1 CNPq Universal and 9974.56.27437.0604/2016 FAPDF.

[*]Corresponding author.

[1]Author partially supported by CNPq.

ACCEPTED MANUSCRIPT

commutative (AC) equational theories. We state the IDP as a restricted higher-order equational unification problem, which we solve using term rewriting techniques and results in AC-matching and linear Diophantine equations. The term "locally stable" comes from the fact that the study of reductions on "small" terms is enough to predict the behaviour of terms under general rewriting; this result is known as the *lifting lemma*.

To obtain the lifting result and to find a subclass of locally stable theories for which the decidability of IDP has a better complexity, we propose an equational reformulation of the class of locally stable theories proposed in [1]. Specifically, we consider a normalised saturation set that takes into account normal contexts and a special set of subterms; we thus obtain the class of **N**-*locally stable* theories.

Our main contributions are:

- *an equational reformulation of the approach proposed in [1] to decide the IDP, based on solving equations modulo the theory embedded in the cryptographic protocol;*
- *a new algorithm for deciding the IDP in the context of* **N**-*locally stable theories;*
- *a more efficient version of the algorithm for the subclass of* **N**-*locally stable theories where inverses are defined, namely, the* **I**-*locally stable theories — we illustrate its use for Abelian Groups (AG), Abelian Groups extended with exponentiation and XOR.*

The new decision algorithm we provide to solve the IDP for **N-** and **I-**locally stable AC-theories (based on a new definition of the saturated set built from the initial knowledge of the intruder), avoids computing AC-congruence classes of terms. It uses an algorithm to solve systems of linear Diophantine equations (SLDE) [12, 17, 26, 40], which we combine with a polynomial algorithm to solve a restricted case of the AG-unification problem [7].

For the **N**-locally stable theories where each AC function symbol $\oplus$ has an inverse $i_{\oplus}$, that is, **I**-locally stable theories, our decision algorithm for the IDP is polynomial on the size of the saturated set, thanks to the use of an algorithm for solving SLDE over $\mathbb{Z}$ (avoiding an exponential time search over the solution space).

We prove that Pure AC theories are **N**-locally stable, and in this case the decision algorithm boils down to solving a system of linear Diophantine equations over naturals (a special case of *Integer Programming Problem*, a well-known NP problem), agreeing with previous complexity results [32]. We show that the theory of Abelian Groups and its extension with exponentiation are **I**-locally stable, and the method is also applicable to the equational theory of XOR (although its signature does not contain a function symbol representing *inverse*, thanks to the axiom $x \oplus x = 0$, where $\oplus$ is the XOR operator, one can classify this theory as an **I**-locally stable theory). This shows that the method proposed is strong enough to deal with a variety of equational theories in a uniform way, unlike previous methods which usually had to be adapted to deal with more complex theories.

Preliminary results have been presented at LSFA 2012 [5], but here we give a new decidability algorithm for the IDP, which runs in polynomial (resp. non-deterministic polynomial) time w.r.t. the size of the saturation set for **I**-locally stable (resp. **N**-locally stable) theories. The complexity results are obtained via a reduction to a restricted case of ground AG-unification (resp. AC-unification) combined with an algorithm to solve SLDE over $\mathbb{Z}$ (resp. $\mathbb{N}$). Moreover, we show that it is possible to apply this methodology to a variety of equational theories: Abelian Groups, Abelian Groups with exponentiation, XOR and Pure AC. We provide AC-convergent rewrite systems and build saturated sets for each of these classes of theories. Abelian Groups,

ACCEPTED MANUSCRIPT

Abelian Groups with Exponentiation and XOR are proven to be **I**-locally stable, and the IDP is decidable in polynomial time on the size of the saturation set. This work is part of the third author's *PhD Thesis* [36].

We address the reader to Section 7 (Related Work) for a comparison with other papers that have investigated the IDP for these equational theories.

Outline of the paper. Section 2 introduces notations and basic definitions used throughout the paper. Section 3 introduces the deduction problem as well as the first equational charaterisation of the deducible terms. Section 4 introduces the class of **N**-*locally stable theories*. Section 5 introduces the class of **I**-*locally stable theories* and presents the decidability algorithm for IDP (Theorem 14). Section 6 presents applications. In Section 7 we present a detailed example to highlight the differences between our algorithm and the one in [1], and discuss other related work. Section 8 concludes the paper. To improve readability, we have omitted some proofs, which can be found in the Appendix together with additional examples.

2. Preliminaries

Standard rewriting notation and notions are used (see e.g. [6]). We assume the following sets: a countably infinite set $\mathcal{N}$ of *names* (we use a, b, c, m to denote names) partitioned into a set $\tilde{n}$ of private names and $\mathcal{PN} = \mathcal{N} - \{\tilde{n}\}$ of public names; a countably infinite set X of *variables* (we use x, y, z to denote variables); and a finite *signature* Σ, consisting of function names and their arities. We write $arity(f)$ for the arity of a function f, and $ar(\Sigma)$ for the maximal arity of a function symbol in Σ.

To represent messages exchanged between participants in a protocol during its execution we will use terms built out of names (representing principal names, nonces, keys, constants involved in the protocol, etc.), variables and function symbols.

Definition 1 (Term)**.** *The set of* terms *over* $\Sigma, X, \mathcal{N}$*, written* $T(\Sigma, X \cup \mathcal{N})$ *is generated by the following grammar:*

$$M, N := a \mid x \mid f(M_1, \ldots, M_n)$$

where f *ranges over the function symbols of* Σ *and* n *matches the arity of* f*,* a *denotes a name (name of parties, public keys, etc.) in* $\mathcal{N}$ *and* x *a variable in* X*.*

We denote by $V(M)$ (resp. $names(M)$) the set of variables (resp. names) occurring in M, and by $pn(M)$ the set of public names occurring in M. We denote by $pn(\Gamma)$ the set of public names occurring in a set Γ of terms. A message M is *ground* if $V(M) = \emptyset$. The *size* $|M|$ of a term M is defined by $|M| = 1$, if M is a name or a variable; and $|f(M_1, \ldots, M_n)| = 1 + \sum_{i=1}^{n} |M_i|$.

The set of *positions* of a term M, denoted by $\mathcal{P}os(M)$, is defined by $\mathcal{P}os(M) := \{\epsilon\}$, if M is a name or a variable; and $\mathcal{P}os(M) := \{\epsilon\} \cup \bigcup_{i=1}^{n} \{ip \mid p \in \mathcal{P}os(M_i)\}$, if $M = f(M_1, \ldots, M_n)$ where $f \in \Sigma$. The position ϵ is called the *root* position. The size of M coincides with the cardinality of $\mathcal{P}os(M)$. The set of *syntactic subterms* of M is defined as $st(M) = \{M|_p \mid p \in \mathcal{P}os(M)\}$, where $M|_p$ denotes the subterm of M at position p. For a set Γ of terms, the notion of a syntactic subterm can be extended as usual: $st(\Gamma) := \bigcup_{M \in \Gamma} st(M)$ (we use the same notation for the subterms of one term or of a set of terms). For $p \in \mathcal{P}os(M)$, we denote by $M[t]_p$ the term that is obtained from M by replacing the subterm at position p by t.

Notice that when the signature Σ contains function symbols that are associative and commutative, the notion of subterms is *dynamic* (it may change modulo AC) and not *static* (as for syntactic subterms). We illustrate it with an example.

ACCEPTED MANUSCRIPT

Example 1. Let t be the term $(f(a + b) + c) + d$, where $+$ is an associative and commutative function symbol, f is a function symbol that is neither commutative nor associative, and a, b, c, d are constants. The set $st(t)$ of *syntactic subterms* of t is: $st(t) = \{t, f(a + b) + c, f(a + b), a + b, a, b, c, d\}$. However, $t =_{AC} t' = f(a + b) + (c + d)$ and in this case, the set of syntactic subterms is $st(t') = \{t', f(a + b), c + d, a + b, a, b, c, d\}$. Thus, for each term in the congruence class of t modulo associativity and commutativity, we may have a different set of syntactic subterms.

Later we will define a notion of subterm st_E that depends on the equational theory under consideration.

Definition 2 (Rewriting system)**.** *A term rewriting system (TRS) is a set $\mathcal{R}$ of oriented equations over terms in a given signature. For terms s and t, $s \to_{\mathcal{R}} t$ denotes that s rewrites to t using a rewriting rule in $\mathcal{R}$, that is, there exist a rule $l \to r \in \mathcal{R}$, a position $p \in \mathcal{P}os(s)$ and a substitution σ such that $s|_p = l\sigma$ and $t = s[r\sigma]_p$. The transitive, reflexive-transitive and equivalence closures of $\to_{\mathcal{R}}$ are denoted by $\overset{+}{\to}_{\mathcal{R}}$, $\overset{*}{\to}_{\mathcal{R}}$ and $\overset{*}{\leftrightarrow}_{\mathcal{R}}$, respectively. The equivalence closure of the rewriting relation, $\overset{*}{\leftrightarrow}_{\mathcal{R}}$, is denoted by $\approx_{\mathcal{R}}$.*

For every term s, the set $s{\downarrow_{\mathcal{R}}}$ of normal forms of s is the set of terms t such that $s \overset{*}{\to}_{\mathcal{R}} t$ and t is irreducible for $\to_{\mathcal{R}}$. $\mathcal{R}$ is said to be convergent whenever it is terminating (for every term t, there is no infinite sequence of the form: $t \to_{\mathcal{R}} t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} \dots$) and confluent (for terms t, u_1 and u_2 such that $t \overset{*}{\to}_{\mathcal{R}} u_1$ and $t \overset{*}{\to}_{\mathcal{R}} u_2$, there exists a term v such that $u_1 \overset{*}{\to}_{\mathcal{R}} v \overset{*}{\leftarrow}_{\mathcal{R}} u_2$).

Definition 3 (Rewriting modulo AC)**.** *Given a TRS $\mathcal{R}$ for which some function symbols are assumed to be AC, and two terms s and t, $s \to_{\mathcal{R}\cup AC} t$ if there exists w such that $s =_{AC} w$ and $w \to_{\mathcal{R}} u$ and $u =_{AC} t$, where $=_{AC}$ denotes equality modulo AC (according to the AC assumption on function symbols).*

For every term s, the set $s{\downarrow_{\mathcal{R}}}$ of normal forms (closed modulo AC) of s is the set of terms t such that $s \overset{*}{\to}_{\mathcal{R}\cup AC} t$ and t is irreducible for $\to_{\mathcal{R}\cup AC}$.

$\mathcal{R}$ is said to be AC-convergent whenever it is AC-terminating (that is, for every term t, there is no infinite sequence of the form: $t \to_{\mathcal{R}\cup AC} t_1 \to_{\mathcal{R}\cup AC} t_2 \dots$) and AC-confluent (that is, for terms t, u_1 and u_2 such that $t \overset{*}{\to}_{\mathcal{R}\cup AC} u_1$ and $t \overset{*}{\to}_{\mathcal{R}\cup AC} u_2$, there exist terms v_1 and v_2 such that $u_1 \overset{*}{\to}_{\mathcal{R}\cup AC} v_1$, $u_2 \overset{*}{\to}_{\mathcal{R}\cup AC} v_2$ and $v_1 =_{AC} v_2$. We denote by $\approx_{\mathcal{R}\cup AC}$ the equivalence closure of $\to_{\mathcal{R}\cup AC}$, that is $\overset{*}{\leftrightarrow}_{\mathcal{R}\cup AC}$.

Definition 4. *We equip the signature Σ with an equational theory $\approx_E$ induced by a set of Σ-equations E, that is, $\approx_E$ is the smallest equivalence relation that contains E and is closed under substitution and compatible with Σ-contexts. An equational theory $\approx_E$ is said to be equivalent to a TRS $\mathcal{R}$ if $\approx_{\mathcal{R}} = \approx_E$, or $\approx_{\mathcal{R}\cup AC} = \approx_E$ if E contains AC axioms.*

*An equational theory $\approx_E$ is convergent when it has an equivalent rewrite system $\mathcal{R}$ which is convergent. Similarly, an equational theory $\approx_E$ is said to be AC-*convergent *when it has an equivalent rewrite system $\mathcal{R}$ that is AC-convergent.*

In the next sections, given an *AC*-convergent equational theory $\approx_E$, normal forms of terms are computed with respect to the TRS $\mathcal{R}$ associated to $\approx_E$, unless otherwise specified. To simplify the notation we will denote by E the equational theory induced by the set of Σ-equations E. We will denote by Σ_E the signature used in the set of equations E.

Definition 5 (Size of the theory E)**.** *The* size *c_E of an equational theory E with an associated TRS $\mathcal{R}$ with rules $\bigcup_{i=1}^{k}\{l_i \to r_i\}$ is defined as $c_E = max_{1\le i\le k}\{|l_i|, |r_i|, ar(\Sigma_E) + 1\}$. For $\mathcal{R} = \emptyset$, define $c_E = ar(\Sigma_E) + 1$.*

ACCEPTED MANUSCRIPT

Definition 6 (Σ-context)**.** *Let $\Box$ be a new symbol that does not occur in $\Sigma \cup X \cup \mathcal{N}$. A* Σ-context *is a term $t \in T(\Sigma, X \cup \mathcal{N} \cup \{\Box\})$ and can be seen as a term with "holes", represented by $\Box$, in it. Contexts are denoted by C. If $\{p_1, \ldots, p_n\} = \{p \in \mathcal{P}os(C) \mid C|_p = \Box\}$, then $C[t_1 \ldots, t_n]$ denotes $C[t_1]_{p_1} \ldots [t_n]_{p_n}$ where we assume the positions $p_1, \ldots, p_n$ are lexicographically ordered. The empty context is a single hole $\Box$.*

In the rest of the paper, a context such that all the function symbols are in Σ_E will be called an *E-context*; $names(C)$ is the set of names occurring in the context C.

Definition 7 (Normal E-context)**.** *Let $\approx_E$ be a convergent equational theory and let $\mathcal{R}_E$ be the associated TRS. Let C be an E-context with n holes and let C_T be the term obtained from C by replacing each hole $\Box$ with a fresh variable $x_1, \ldots, x_n$, where $x_i \neq x_j$, for $i \neq j$ $(1 \leq i, j \leq n)$. The E-context C is said to be* normal *if, and only if, C_T cannot be reduced via the TRS $\mathcal{R}_E$.*

This concept can be extended to AC-convergent rewrite systems in the usual way.

Example 2. Consider the signature $\Sigma_{AG} = \{+, i, 0\}$ for Abelian Groups.

The equational theory for Abelian Groups and the associated TRS are

$$E_{AG} = \begin{cases} x + (y + z) = (x + y) + z \\ x + y = y + x \\ x + 0 = x \\ x + i(x) = 0 \\ i(x + y) = i(x) + i(y) \end{cases} \qquad \mathcal{R}_{AG} = \begin{cases} x + 0 \to x & (1) \\ x + i(x) \to 0 & (2) \\ i(i(x)) \to x & (3) \\ i(0) \to 0 & (4) \\ i(x + y) \to i(x) + i(y) & (5) \end{cases}$$

$\mathcal{R}_{AG}$ is AC-convergent (see Proposition 16).

Let C be the Σ_{AG}-context $i(0) + \Box$. Notice that the E_{AG}-context C is not *normal*; it reduces using rules (4) and (1) as follows: $i(0) + \Box \to 0 + \Box \to \Box$. The E_{AG}-context $\Box$ is *normal*.

Notice that the Σ_{AG}-context $C' = i(\Box) + \Box$ is normal: if the holes are replaced with x_1, x_2, the reduction via rule $i(x) + x \to 0$ is not possible.

In the rest of the paper, we use signatures, terms and equational theories to model protocols. As mentioned earlier, *messages* are represented by terms. Equational theories and rewriting systems are used to model the cryptographic primitives in the protocol and the algebraic capabilities of an intruder. Unless stated otherwise, for the next results, the terms are ground. We write $M == N$ to denote syntactic equality of ground terms.

3. Deduction Problem

Given a set Γ that represents the information observed by an attacker during a communication, we may ask whether a given ground term M may be deduced from Γ using equational reasoning. This relation is written $\Gamma \vdash M$ and axiomatised in a natural-deduction style, using the inference rules given in Table 1.

Note that the intruder is able to use public names in its reasoning, via rule $(Ax)_{Pu}$: the intruder can deduce the name s whenever $s \notin \tilde{n}$ [2].

Proposition 1 gives an equational characterisation[3] of the terms that can be deduced from Γ. It states that the IDP is equivalent to the problem of finding a context C such that $names(C) \cap \tilde{n} = \emptyset$

[2] This is an attempt to represent the power given to the intruder in [1].

[3] A similar charaterisation is given in [42, 23].

ACCEPTED MANUSCRIPT

Table 1: System $\mathfrak{R}$: a natural deduction system for intruder equational deduction

$$\frac{M \in \Gamma}{\Gamma \vdash M}\ (id) \qquad \frac{}{\Gamma \vdash s}\ (Ax)_{Pu},\ s \in \mathcal{N} - \tilde{n}$$

$$\frac{\Gamma \vdash M_1 \quad \ldots \quad \Gamma \vdash M_n}{\Gamma \vdash f(M_1, \ldots, M_n)}\ (f_I)\ f \in \Sigma \qquad \frac{\Gamma \vdash N}{\Gamma \vdash M}\ (\approx)\ M \approx_E N$$

and $C[M'_1, \ldots, M'_n] \approx_E M$ for terms $M'_1, \ldots, M'_n \in \Gamma$. The latter is a restricted case of a higher-order unification problem modulo an equational theory. Before stating the property, we introduce the notion of S^E*-constructible term*

Definition 8 (S^E-constructibility)**.** *Given a set S of ground terms, a set $\tilde{n}$ of private names and an equational theory E, we say that a term M is* S^E-constructible *if there exists a context C such that names$(C) \cap \tilde{n} = \emptyset$ and $T_1, \ldots, T_k \in S$ such that $M \approx_E C[T_1, \ldots, T_k]$.*

Proposition 1. *Let E be an equational theory, M a ground term, $\Gamma = \{M_1, \ldots, M_n\}$ a finite set of ground terms and $\tilde{n}$ a set of private names. Then $\Gamma \vdash M$ if and only if M is Γ^E- constructible.*

Proof. ($\Rightarrow$) The proof is by induction on the derivation $\mathcal{D}$ of $\Gamma \vdash M$:

Base Case. $\Gamma \vdash M$ has been obtained via an application of (id) or $(Ax)_{Pu}$. In the first case, $M \in \Gamma$ and $C[M] \approx_E M$ for the empty context C. In the second case, $M \in N - \{\tilde{n}\}$, and the result follows trivially.

Induction Step. We distinguish cases depending on the last rule applied.

1. The rule applied is (f_I)

$$\frac{\dfrac{\mathcal{D}_1}{\Gamma \vdash M_1} \quad \ldots \quad \dfrac{\mathcal{D}_r}{\Gamma \vdash M_r}}{\Gamma \vdash M = f(M_1, \ldots, M_r)}\ (f_I)$$

   By IH, $M_i \approx_E C_i[M_{i1}, \ldots, M_{in_i}]$ for contexts C_i and terms $M_{i_j} \in \Gamma$, $1 \leq i \leq r$ and $1 \leq j \leq n_i$. Therefore, $M \approx_E f(C_1[M_{11}, \ldots, M_{1n_1}], \ldots, C_r[M_{r1}, \ldots, M_{rn_r}]) = C^*[M_1, \ldots, M_t]$ for some context C^* and terms $M_1, \ldots, M_t \in \Gamma$ and the result follows.

2. The rule applied is $\approx_E$ Then

$$\frac{\dfrac{\mathcal{D}'}{\Gamma \vdash N}}{\Gamma \vdash M} \approx_E$$

   By IH, $N \approx_E C[M_1, \ldots, M_t]$ for some context C and terms $M_1, \ldots, M_t \in \Gamma$. Since $N \approx_E M$ the result follows.

($\Leftarrow$) Suppose that $M \approx_E C[M_1, \ldots, M_r]$ for a context C and terms $M_1, \ldots, M_r \in \Gamma$. By definition, C is formed using only function symbols of the signature Σ_E and its size is finite. Therefore, after a finite number of applications of rules (f_I) and $(\approx_E)$ (represented by rule (F)) we have:

ACCEPTED MANUSCRIPT

$$\dfrac{\dfrac{M_1 \in \Gamma}{\Gamma \vdash M_1}\,(id) \quad \ldots \quad \dfrac{s_1 \in N - \{\tilde{n}\}}{\Gamma \vdash M_1}\,(Ax)_{Pu} \quad \ldots \quad \dfrac{M_r \in \Gamma}{\Gamma \vdash M_r}\,(id)}{\Gamma \vdash M}\,(F)$$

□

In the following, a method for solving this equational unification problem will be studied.

4. Locally Stable Theories

Abadi and Cortier [1] propose a method to deal with the deducibility relation for a class of *locally stable* theories. The idea is to compute a *saturation set* for a given set Γ of terms (the intruder's knowledge), by considering sums of terms that can be built by the intruder and normal contexts formed with symbols of the signature and public names.

Definition 9. *Let $\oplus$ be an arbitrary AC function symbol in Σ_E for an equational theory E. We write $\alpha \cdot_\oplus M$ for the term $M \oplus \ldots \oplus M$, α times ($\alpha \in \mathbb{N}$). Given a set S of terms and a set $\tilde{n}$ of private names, write $sum_\oplus(S, \tilde{n})$ for the set of arbitrary sums of terms in S and other names:*

$$sum_\oplus(S, \tilde{n}) = \left\{ \begin{array}{l|l} (\alpha_1 \cdot_\oplus T_1) \oplus \ldots \oplus (\alpha_r \cdot_\oplus T_r) \oplus & \alpha_i, \beta_j \in \mathbb{N} - \{0\} \\ (\beta_1 \cdot_\oplus m_1) \oplus \ldots \oplus (\beta_k \cdot_\oplus m_k) & r, k \in \mathbb{N} \\ & T_i \in S, m_i \in \mathcal{PN} \end{array} \right\}$$

Define $sum(S, \tilde{n}) = \bigcup_{i=1}^{k} sum_{\oplus_i}(S, \tilde{n})$, where $\oplus_1, \ldots, \oplus_k$ are the AC-symbols of the theory.

In the following results we will be interested in applications of rewrite rules in the head of terms (modulo AC):

Definition 10. *Given an AC-convergent rewriting system $\mathcal{R}$ the* head rewrite *relation $\xrightarrow{h}$ is defined as $s \xrightarrow{h} t$* iff there exist a rule $l \to r \in \mathcal{R}$ and a substitution θ such that

- *either $s =_{AC} l\theta$ and $t = r\theta$;*
- *or there exist terms s_1 and s_2 such that $s =_{AC} s_1 \oplus s_2$, $s_1 =_{AC} l\theta$ and $t =_{AC} r\theta \oplus s_2$.*

The class of *locally stable theories* was defined in [1] within the framework of the applied pi-calculus; we recall the definition below, where we write $[S]_{AC}$ for the closure of S modulo AC.

Definition 6 in [1]. *An AC-convergent equational theory E is* locally stable *if, for any frame $\phi = \nu\tilde{n}.\{M_1/x_1, \ldots, M_k/x_k\}$, where the terms M_i are closed and in normal form, there exists a finite (computable) set $sat(\phi)$ closed modulo AC (i.e. $sat(\phi) = [sat(\phi)]_{AC}$), such that*

1. *$M_1, \ldots, M_k \in sat(\phi)$, and $n \in sat(\phi)$ for every $n \in fn(\phi)$;*
2. *if $M_1, \ldots, M_k \in sat(\phi)$ and $f(M_1, \ldots, M_k) \in st(sat(\phi))$, then $f(M_1, \ldots, M_k) \in sat(\phi)$, where $f \in \Sigma$;*
3. *if $C[S_1, \ldots, S_l] \xrightarrow{h} M$, where C is a context such that $|C| \leq c_E$ and $fn(C) \cap \tilde{n} = \emptyset$, and where $S_1, \ldots, S_l \in sum_\oplus(sat(\phi), \tilde{n})$ for some AC-symbol $\oplus$ (or $S_i \in sat(\phi)$ if there is no AC-symbol), then there exist a context C', a term M', and $S'_1, \ldots, S'_k \in sum_\oplus(sat(\phi))$ (or $S'_1, \ldots, S'_k \in sat(\phi)$ if there is no AC-symbol), such that $|C'| \leq c_E^2$, $fn(C') \cap \tilde{n} = \emptyset$, and $M \xrightarrow{*}_{AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$;*

ACCEPTED MANUSCRIPT

4. *if* $M \in sat(\phi)$ *then* $\phi \vdash M$.

The *Lifting Lemma* guarantees that, for locally stable theories, the local analysis of terms built from $sat(\phi)$ is enough to predict the behaviour of these terms.

Lemma 11 in [1] – Lifting Lemma. *Let E be a locally stable theory. Let* $\phi = \nu\tilde{n}.\sigma$ *be a frame. For every context* C_1 *such that* $fn(C_1) \cap \tilde{n} = \emptyset$*, for every* $M_i \in sat(\phi)$*, for every term T such that* $C_1[M_1, \ldots, M_k] \rightarrow_{AC} T$*, there exist a context* C_2 *such that* $fn(C_2) \cap \tilde{n} = \emptyset$*, and terms* $M'_i \in sat(\phi)$*, such that* $T \rightarrow^*_{AC} C_2[M'_1, \ldots, M'_k]$.

4.1. A counter-example

Below we define an equational theory E_{ex} for which it is possible to build a saturation set satisfying the conditions in Definition 6 in [1][4] and for which the lifting lemma does not hold. In order to facilitate the presentation we will adopt the language established in the preliminaries section instead of the language of the applied pi-calculus.

Equational theory E_{ex}**.** Consider the TRS

$$\mathcal{R}_{ex} = \left\{ \begin{array}{lllll} (r1) & h(f(x,y)) & \rightarrow & h(x+y) \\ (r2) & x+x & \rightarrow & x \end{array} \right.$$

Proposition 2. $\mathcal{R}_{Ex}$ *is convergent modulo associtivity and commutativity of* $+$.

Proof. Termination can be proved by interpreting terms as pairs (size, number of f symbols) and using the lexicographic extension of the standard ordering on natural numbers: $r2$ decreases the size of the term, whereas $r1$ keeps the same size but decreases the number of f symbols. Confluence follows from Newman's lemma since there are no critical pairs. □

For any given set Γ of ground terms in normal form, there exists a saturation set $sat(\Gamma)$ for this theory, which satisfies the conditions specified in Definition 6 in [1]. Recall that $pn(\Gamma)$ denotes the set of public names occurring in Γ.

Definition 11 (Set $sat(\Gamma)$ for E_{ex})**.** *Given a finite set* $\Gamma = \{M_1, \ldots, M_n\}$ *of ground terms in normal form and a finite set* $\tilde{n}$ *of private terms, let* $sat(\Gamma)$ *be the smallest set such that*

1. $\Gamma \subseteq sat(\Gamma)$ *and* $m \in sat(\Gamma)$ *for all* $m \in pn(\Gamma)$*;*
2. *if* $N_1, \ldots, N_k \in sat(\Gamma)$ *and* $g(N_1, \ldots, N_k) \in st(sat(\Gamma))$ *then* $g(N_1, \ldots, N_k) \in sat(\Gamma)$*, where* $g \in \{f, h, +\}$*;*
3. *if* $N \in sat(\Gamma)$ *and* $h(N) \xrightarrow{h} N'$ *via rule* $(r1)$ *then* $N' \in sat(\Gamma)$*;*
4. $N_1, N_2 \in sat(\Gamma)$*,* $N_1 \neq N_2$ *and* $N_1 + N_2 \xrightarrow{h} N'$ *via rule* $(r2)$ *then* $N'' \in sat(\Gamma)$*, where* N'' *is obtained by head reducing* N' *as much as possible with rule* $(r2)$*, hence* $N' \xrightarrow{h*} N''$ *(in case rule* $(r2)$ *does not apply,* $N' \in sat(\Gamma)$*);*

[4] but in case 1 we only put public names in $sat(\phi)$ to ensure deducibility of all the terms in $sat(\phi)$.

ACCEPTED MANUSCRIPT

5. *if* $N_1 =_{AC} N_2$ *and* $N_1 \in sat(\Gamma)$ *then* $N_2 \in sat(\Gamma)$.

Note that, since we are rewriting modulo AC, condition 4 ensures that if $a + b$ and $a + c$ are in $sat(\Gamma)$, then $a + b + c$ is in $sat(\Gamma)$ too.

The set defined above is finite and satisfies the required conditions, therefore E_{ex} is locally stable according to Definition 6 in [1].

Problem Case. Consider the set $\Gamma = \{f(m, m)\}$ where $\tilde{n} = \{m\}$. The set $sat(\Gamma)$ generated for E_{ex} using Definition 11 is $sat(\Gamma) = \{f(m, m), h(m + m)\}$. Note that

- $f(m, m) \in sat(\Gamma)$ by condition 1 in Definition 11, and $h(m + m) \in sat(\Gamma)$ by condition 3 in Definition 11 because $h(f(m, m)) \xrightarrow{h} h(m + m)$.

Notice also the following: since $h(f(m, m)) \xrightarrow{h} h(m + m)$, by condition 3 in the definition of locally stable theories, there exist a context C', a term M' and terms $S_1, \ldots, S_l \in sum(sat(\Gamma), \tilde{n})$ such that $h(m + m) \xrightarrow{*} M' =_{AC} C'[S_1, \ldots, S_l]$.

This is true: C' is the empty context, $M' = h(m + m) \in sat(\Gamma) \subseteq sum(sat(\Gamma), \tilde{n})$ (we use zero steps of reductions).

However, the Lifting Lemma does not hold: from the term $h(m + m) \in sat(\Gamma)$ there is a non-head reduction $h(m + m) \to h(m)$ and there are no terms in $sat(\Gamma)$ and context C such that $h(m) \to^*_{AC} C[S_1, \ldots, S_k]$.

We conjecture that closing by normal forms the set $sat(\Gamma)$ defined in [1] (Definition 6) solves the problem. However, adding normal forms of terms in the definition of $sat(\Gamma)$ might affect the class of theories defined. By introducing new terms in $sat(\Gamma)$, conditions 2 and 3 may be affected (we may have new terms that can be head-reduced when combined with other terms, and in the worst case scenario, an infinite number of new terms could be generated).

4.2. Normal Locally Stable Theories

We now consider a variant of Definition 6 in [1] for which we can prove the lifting lemma. We propose the following modifications in the definition of $sat(\Gamma)$ given in [1]:

1. the set $sat(\Gamma)$ will be closed under normal forms;
2. the contexts considered in $sat(\Gamma)$ will be normalised;
3. the set of subterms used in $sat(\Gamma)$ will be defined according to the equational theory E;
4. the set $sat(\Gamma)$ will not be closed modulo AC (we push this to the decidability algorithm).

These modifications play an important role in our proof of *Lifting* (Lemma 3), which guarantees that analysing reduction locally gives a characterisation of general reduction on terms. Additionally, it will help to bound the size of the saturation set $sat(\Gamma)$.

In the rest of the paper, this reformulated notion of locally stable theory will be called **N**-*locally stable* (or *normal* locally stable). We give the definition below, observing that the notion of subterm depends on the equational theory E under consideration. Subterms will be computed using a function st_E, which should satisfy the following property:

1. $st_E(u) \subseteq st_E(T)$, whenever $u \in st_E(T)$, where T is a set of terms (again we use the same notation for subterms of one term and subterms of a set of terms).

ACCEPTED MANUSCRIPT

Definition 12 (**N**-Locally Stable Theory)**.** *An AC-convergent equational theory E, with a given subterm function st_E, is* **N**-locally stable *if, for every finite set $\Gamma = \{M_1, \ldots, M_n\}$ of ground terms in normal form together with a set $\tilde{n}$ of private names, there exists a finite and computable set $sat(\Gamma)$ such that*

1. $\Gamma \subseteq sat(\Gamma)$ *and* $m \in sat(\Gamma)$ *for every* $m \in pn(\Gamma)$*;*
2. *if* $N_1, \ldots, N_k \in sat(\Gamma)$ *and* $f(N_1, \ldots, N_k) \in st_E(sat(\Gamma))$ *then* $f(N_1, \ldots, N_k) \in sat(\Gamma)$*, for* $f \in \Sigma_E$*;*
3. *if* $C[S_1, \ldots, S_l] \xrightarrow{h} M$*, where C is an AC-normal context such that* $names(C) \cap \tilde{n} = \emptyset$ *and* $|C| \leq c_E$*, and* $S_1, \ldots, S_l \in sum_{\oplus}(sat(\Gamma), \tilde{n})$*, for some AC symbol* $\oplus$*, then there exist an AC-normal context* C' *with* $names(C') \cap \tilde{n} = \emptyset$*, a term* M' *and terms* $S'_1, \ldots, S'_k \in sum_{\oplus}(sat(\Gamma), \tilde{n})$*, such that* $M \xrightarrow{*}_{\mathcal{R} \cup AC} M' =_{AC} C'[S'_1, \ldots, S'_k]$*;*
4. *if* $M \in sat(\Gamma)$ *then* $M{\downarrow} \in sat(\Gamma)$ [5]*.*
5. *if* $M \in sat(\Gamma)$ *then* $\Gamma \vdash M$*.*

The set $sat(\Gamma)$ may not be unique. Any set $sat(\Gamma)$ satisfying the five conditions is adequate for the results. The AC-normal contexts used in condition 3 are built from symbols from Σ and public names, this represents the construction obtained from System $\mathfrak{R}$, after some number of applications of rule (f_l) in Table 1.

Notice that with this definition of **N**-locally stable theory, the existence of AC-symbols in the signature Σ_E does not necessarily imply an exponential size for $sat(\Gamma)$ with relation to the size of Γ, as it was in [1], since we are not closing the saturation set modulo AC.

Lemma 3 (Lifting)**.** *Let E be an* **N***-locally stable theory, $\Gamma = \{M_1, \ldots, M_n\}$ a set of ground terms in normal form and $\tilde{n}$ a set of private names. For every context C_1 such that* $names(C_1) \cap \tilde{n} = \emptyset$*, for every* $T_1, \ldots, T_k \in sat(\Gamma)$*, for every term T such that* $C_1[T_1, \ldots, T_k] \rightarrow_{\mathcal{R} \cup AC} T$*, there exists an AC-normal context* C_2 *with* $names(C_2) \cap \tilde{n} = \emptyset$*, and terms* $T'_1, \ldots, T'_l \in sat(\Gamma)$*, such that* $T \xrightarrow{*}_{\mathcal{R} \cup AC} C_2[T'_1, \ldots, T'_l]$*.*

Proof. A complete proof can be found in the Appendix. Here we show the point where the addition of normal forms in $sat(\Gamma)$ helps us to prove this lemma.

Suppose that $C_1[T_1, \ldots, T_k] \rightarrow_{AC} T$, for a normal context C_1 and terms $T_1, \ldots, T_k \in sat(\Gamma)$. Notice that, since E is AC-convergent, every context can be normalised. If the reduction were to happen in a term T_i, then two cases would be possible:

- if $T_i \xrightarrow{h} T'_i$ then, by condition 3 of Definition 12, the result would follow, that is, $T'_i \xrightarrow{*} C'[S'_1, \ldots, S'_n] =_{AC} C''[T''_1, \ldots, T''_k]$, for $S'_j \in sum_{\oplus}(sat(\Gamma), \tilde{n})$ and $T''_j \in sat(\Gamma)$.
- if $T_i \rightarrow T'_i$ in a position different from the head then the previous definition locally stable theories [1] has nothing to say about the structure of the term. However, according to the definition of **N**-locally stable theories (Definition 12), for every $T \in sat(\Gamma)$, $T{\downarrow} \in sat(\Gamma)$, therefore: $T'_i \xrightarrow{*} T_i{\downarrow} = C[T_i{\downarrow}]$ for an empty context C and $T_i{\downarrow} \in sat(\Gamma)$.

[5] We only add one representative modulo AC of $M{\downarrow}$ in $sat(\Gamma)$

ACCEPTED MANUSCRIPT

□

Corollary 4. *Let E be an **N**-locally stable theory. Let $\Gamma = \{M_1, \ldots, M_n\}$ be a set of ground terms in normal form and $\tilde{n}$ a set of private names. For every AC-normal context C_1 with $names(C_1) \cap \tilde{n} = \emptyset$, for every $T_1, \ldots, T_k \in sat(\Gamma)$, for every T in normal form such that $C_1[T_1, \ldots, T_k] \xrightarrow{*}_{\mathcal{R} \cup AC} T$, there exists an AC-normal context C_2 with $names(C_2) \cap \tilde{n} = \emptyset$ and terms $T'_1, \ldots, T'_l \in sat(\Gamma)$ such that $T =_{AC} C_2[T'_1, \ldots, T'_l]$, i.e., T is $sat(\Gamma)^{AC}$-constructible.*

In the following we show that any term M deducible from Γ is equal modulo AC to a context over terms in $sat(\Gamma)$. This Lemma is similar to Proposition 16 in [1], here we check for $=_{AC}$ instead of == (that is, equality modulo AC instead of syntactic equality).

Lemma 5. *Let E be an **N**-locally stable theory. Let $\Gamma = \{M_1, \ldots, M_n\}$ be a finite set of ground terms in normal form, $\tilde{n}$ a set of private names and M a ground term in normal form. Then $\Gamma \vdash M$ if and only if M is $sat(\Gamma)^{AC}$-constructible.*

As a consequence of the previous results, we obtain the decidability of IDP for **N**-locally stable theories: To decide whether M is deducible from Γ or not, it is sufficient to check whether there exists a context C with $names(C) \cap \tilde{n} = \emptyset$, and terms $T_1, \ldots, T_k \in sat(\Gamma)$, such that $C[T_1, \ldots, T_k] =_{AC} M$ (we provide the decision algorithm in Lemma 15 below).

Theorem 6. *The IDP is decidable for **N**-locally stable theories.*

4.3. Application: Pure AC Theories

We now show that the AC equational theory is **N**-locally stable; we can then conclude that for pure *AC* theories the IDP is decidable. We show in Section 5 that it is in NP, agreeing with previous results [32].

Consider the signature Σ_{AC} which contains only constant symbols and the *AC*-symbol $\oplus$. The equational theory E_{AC} contains only the *AC* equations for $\oplus$:

$$E_{AC} = \left\{ \; x \oplus y = y \oplus x \qquad\qquad x \oplus (y \oplus z) = (x \oplus y) \oplus z \; \right\}$$

In this case, $\mathcal{R} = \emptyset$ is the *AC*-convergent TRS associated with E_{AC}.

In the following definition, a notion of subterms st_{AC} adequate for the theory *AC*-pure will be introduced, this notion takes into account possible combinations of terms modulo AC of $\oplus$:

Definition 13 (Atom)**.** *Let u be a term, we define $atoms(u)$ as*

- *if $u = u_1 \oplus u_2 \oplus \ldots \oplus u_q$, where each u_i is flattened w.r.t $\oplus$, then $atoms(u) = \{u_1, \ldots, u_q\}$.*
- *if u is not headed with $\oplus$, then $atoms(u) = \{u\}$.*

This notion of terms can be extended for a set T of terms: $atoms(T) := \bigcup_{t \in T} atoms(t)$.

Definition 14 ($S_{AC}(t)$)**.** *Let t be a ground term in normal form. Define $S_{AC}(t)$ as $t \in S_{AC}(t)$ and if $u = u_1 \oplus u_2 \oplus \ldots \oplus u_n \in S_{AC}(t)$ then $atoms(u) \in S_{AC}(t)$.*

This notion of subterms can be extended for a set T of ground terms in normal form in the usual way: $S_{AC}(T) := \bigcup_{t \in T} S_{AC}(t)$.

ACCEPTED MANUSCRIPT

For example, if $t = a \oplus b \oplus c$ then $S_{AC}(t) = \{t, a, b, c\}$.

The set below consists of all linear combinations over $\mathbb{N}$ of atoms in a set T of ground terms in normal form.

Definition 15 ($SS_{AC}(T)$)**.** *Let T be a finite set of ground terms in normal form. Define $SS_{AC}(T)$ as the set* $SS_{AC}(T) := \left\{ \bigoplus_{s \in M} \alpha_s \cdot s \mid M \subseteq S_{AC}(T), \alpha_s \in \mathbb{N} \right\}$.

The set below is a subset of the terms in $SS_{AC}(T)$ which are subterms from T.

Definition 16 ($st_{AC}(T)$)**.** *Let T be a finite set of ground terms in normal form. Define $st_{AC}(T)$ as*

$$st_{AC}(T) := \{M \in SS_{AC}(T) \mid M =_{AC} t|_p, \text{ for a term } t \in S_{AC}(T) \text{ and some } p \in \mathcal{P}os(t)\} \cup S_{AC}(T)$$

Notice that the set $st_{AC}(T)$ will contain atoms from T, repeated copies of these atoms, sums of two atoms, three atoms, etc., as long as these terms are subterms from T modulo AC.

Example 3. Let $t = 2a \oplus 3b \oplus 3c$ be a ground term. By definition, $atoms(t) = \{a, b, c\}$ and $SS_{AC}(t) = \{\alpha_a \cdot a \oplus \alpha_b \cdot b \oplus \alpha_c \cdot c \mid \alpha_j \in \mathbb{N}, j = a, b, c\}$. In addition,

$$st_{AC}(t) = \{\alpha_a \cdot a \oplus \alpha_b \cdot b \oplus \alpha_c \cdot c \mid 0 \leq \alpha_a \leq 2,\ 0 \leq \alpha_b, \alpha_c \leq 3\}$$

whose size is $\sum_{j=a,b,c} |t|_j + \sum_{j \neq i} |t|_i \cdot |t|_j + (|t|_a \cdot |t|_b \cdot |t|_c)$ which is in $O(|t|^3)$, where $|t|_a$ denotes the number of occurrences of a in t.

Reasoning similarly, $|st_{AC}(T)|$ is in $O(|T|^n)$, with $n = |atoms(T)|$.

Definition 17 ($sat(\Gamma)$ for AC)**.** *Let $\Gamma = \{M_1, \ldots, M_k\}$ be a finite set of ground terms in normal form. Let us define $sat(\Gamma)$ for the pure AC theory as the smallest set such that*

1. *$\Gamma \subseteq sat(\Gamma)$ and $m \in sat(\Gamma)$ for every $m \in pn(\Gamma)$;*
2. *if $N_i, N_j \in sat(\Gamma)$ and $N_i \oplus N_j \in st_{AC}(sat(\Gamma))$ then $N_i \oplus N_j \in sat(\Gamma)$.*

The set $sat(\Gamma)$ is finite since we add only terms whose size is smaller than or equal to the maximal size of the terms in Γ, more specifically, $|sat(\Gamma)|$ is in $O(|T|^n)$, with $n = atoms(\Gamma)$. It is easy to see that the set $sat(\Gamma)$ satisfies conditions 1,2, 4 and 5 in the definition of **N**-locally stable theories. Since $\mathcal{R} = \emptyset$ it follows that condition 3 is also satisfied. Therefore, we have the following result:

Lemma 7. *E_{AC} is normal locally stable.*

By Theorem 6 the Intruder Deduction Problem for pure *AC* is decidable. Moreover, the algorithm we give in Section 5 can also be used to deal with this theory, and we can conclude the problem is in NP.

Theorem 8. *The Intruder Deduction Problem for Pure AC theories is in NP.*

Proof. The algorithm presented in Section 5.2 for **I**-locally stable theories (see Theorem 13) can be used also for **N**-locally stable theories, however, we would have to solve the system of linear Diophantine equations S over $\mathbb{N}$, which is an NP-complete problem [40]. □

ACCEPTED MANUSCRIPT

Remark 1. In particular, for the AC-pure theory, our algorithm will run in non-deterministic polynominal time with relation to $|sat(\Gamma) \cup \{M\}|$, which is polynomial on $|\Gamma \cup \{M\}|$. In [1], the authors provide a polynomial algorithm with relation to $|sat(\Gamma) \cup \{M\}|$, however, their saturation set $sat(\Gamma)$ is exponential on the size of Γ, since they add all the terms in the AC-congruence class of each term in $sat(\Gamma)$.

5. IDP in Locally Stable Theories with Inverses

In this section we focus on a subclass of **N**-locally stable theories for which each *AC* symbol in the signature has an inverse. The goal is to propose a decidability algorithm for IDP using an algorithm to solve systems of linear Diophantine equations (SLDE) over $\mathbb{Z}$ (the inverses will be interpreted as *negative integers*).

5.1. Locally Stable Theories with Inverses

We start by defining a subclass of *AC* equational theories that contains the axioms for Abelian Groups ($ACUI_{\oplus}$).

(*) *In the following results, let E be a theory whose signature* Σ_E *contains, for each AC function symbol* $\oplus$*, its corresponding* inverse $i_{\oplus}$.

More precisely, in the following results, we consider equational theories E containing the equations:

$$UI_{\oplus} = \{x \oplus i_{\oplus}(x) = e_{\oplus} \qquad x \oplus e_{\oplus} = x\}$$

for each AC-symbol $\oplus$ *in* Σ_E*, where* $i_{\oplus}$ *is the unary function symbol representing the inverse of* $\oplus$ *and* $e_{\oplus}$ *is the corresponding neutral element.*

Note that $ACUI_{+}$ is equivalent to the theory E_{AG} given in Example 2 for Abelian Groups. In the rest of the paper, we call the theory with the axioms $ACUI$ simply AG.

Definition 18 (Locally Stable with Inverses)**.** *A* locally stable theory with inverses *E (***I***-locally stable theory for short) is an* **N***-locally stable theory such that*

1. *for each AC symbol* $\oplus$ *in the signature, the rules in* $\mathcal{R}_{AG}$ *are derivable, that is, if* $l \to r$ *is in* $\mathcal{R}_{AG}$ *then* $l \overset{*}{\to}_{\mathcal{R}_E} r$*,*
2. *the set* $sat(\Gamma)$ *(see Definition 12) is closed under inverses: if* $M \in sat(\Gamma)$*, then* $i_{\oplus}(M)\downarrow \in sat(\Gamma)$*.*
3. $sat(\Gamma)$ *is closed under linear combinations, that is, if* $S_1, \ldots, S_n \in sat(\Gamma)$*, then for any* $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$*,* $(\alpha_1 S_1 \oplus \ldots \oplus \alpha_n S_n)\downarrow =_{AC} \beta_1 T_1 \oplus \ldots \oplus \beta_m T_m$*, for some* $T_1, \ldots, T_m \in sat(\Gamma)$*.*

Note that as usual, we do not require the set to be closed under AC, that is, we only add one representative modulo AC of each term.

The presence of inverses in this subclass of the **N**-locally stable theories allows the intruder to compute subterms of the terms previously observed, as the following example shows.

Example 4. Let $\Gamma = \{a + b + c + d, b, m_1, \ldots, m_k\}$ be the set of messages that the intruder has eavesdropped in a communication. In an **I**-locally stable theory, the intruder may compute $(a + b + c + d) + i(b) \to a + c + d$ and this computation gives to the intruder more information. Now, the intruder's knowledge has increased to $\Gamma \cup \{a + c + d\}$.

ACCEPTED MANUSCRIPT

In what follows we want to reason not only modulo associativity and commutativity, but also modulo application of inverses and neutral elements (represented by the indentities in $UI_{\oplus}$).

The following result is a version of Lemma 5 for **I**-locally stable theories. It relates the decidability of the IDP to the decidability of $=_{AG}$ (the latter is decidable in polynomial time in the ground case [7]).

Lemma 9. *Let E be an **I**-locally stable theory. Let $\Gamma = \{M_1, \ldots, M_n\}$ be a finite set of ground terms in normal form, $\tilde{n}$ a set of private names, and M a ground term in normal form. Then $\Gamma \vdash M$ if and only if M is $sat(\Gamma)^{AG}$-constructible.*

Proof. Suppose that $M =_{AG} C[T_1, \ldots, T_k]$ for terms $T_i \in sat(\Gamma)$ and a context C. By Definition 12, $\Gamma \vdash T_i$ and, by Proposition 1, $T_i \approx_E C_i[M_{i1}, \ldots, M_{in_i}]$, for contexts $C_i(names(C_i) \cap \tilde{n} = \emptyset)$ and terms $M_{i1}, \ldots, M_{in_i} \in \Gamma$, $1 \leq i \leq k$. Since $\approx_{AG} \subset \approx_E$ for E an **I**-locally stable theory, it follows that $M \approx_E C[C_1[M_{11}, \ldots, M_{1n_1}], \ldots, C_k[M_{k1}, \ldots, M_{kn_k}]]$, i.e., there exist a context C^* and terms $M_1'', \ldots, M_t'' \in \Gamma$ such that $M \approx_E C^*[M_1'', \ldots, M_t'']$. By Proposition 1, $\Gamma \vdash M$.

Conversely, if $\Gamma \vdash M$ then, by Proposition 1, $M \approx_E C[M_1, \ldots, M_1]$ for a context C and terms $M_1, \ldots, M_k \in \Gamma \subset sat(\Gamma)$. Since M is in normal form, $C[M_1, \ldots, M_k] \xrightarrow{*} M$, applying Corollary 4, there exist a context C_2 and terms $M_1', \ldots, M_k' \in sat(\Gamma)$ such that $M =_{AC} C_2[M_1', \ldots, M_k']$, since $\approx_{AC} \subset \approx_{AG}$ the result follows. □

We prove in Section 6.1 that AG is **N**-locally stable, and also **I**-locally stable.

5.2. Algorithms to decide the IDP for Locally Stable Theories with Inverses

We next show that the IDP for locally stable theories with inverses, which can be seen as a restricted case of higher-order AG-matching ("is there a context C such that $names(C) \cap \tilde{n} = \emptyset$ and $M =_{AG} C[M_1, \ldots, M_k]$ for some $M_1, \ldots, M_k \in sat(\Gamma)$?", or equivalently, "is M $sat(\Gamma)^{AG}$-constructible?"), can be solved in polynomial time in $|sat(\Gamma)|$ and $|M|$ using an algorithm to decide elementary AG-unification with constants [7].

Let E be an **I**-locally stable theory, $\Gamma = \{M_1, \ldots, M_n\}$ a finite set of ground messages in normal form, $\tilde{n}$ a set of private names and M a ground term in normal form. Then the question of whether M is $sat(\Gamma)^{AG}$-constructible can be decided using the following algorithm.

First, we construct the set $sat(\Gamma) = \{T_1, \ldots, T_s\}$, which is computable and finite by Definition 12. We then check whether M is $sat(\Gamma)^{AG}$-constructible by calling `CHECK`$(M, sat(\Gamma))$, using the auxiliary functions `BUILD`, `EXTEND` and `DIOPHANTINE` (defined below in Algorithms 1, 2 and 3, respectively). Intuitively,

- `BUILD` will be called with a term N and a set S of terms, and will return `true` if N can be built using terms from $[S]_{AC}$, public names and function symbols from Σ.
- `EXTEND` takes a term M and a set S of terms and returns an extended set of terms obtained after adding all the constructible sums in M.
- `DIOPHANTINE`(M, S) checks whether M can be written as a linear combination of terms in the set S.
- `CHECK`(M, S)=`BUILD`$(M,$ `EXTEND`(M,S)).
  Given a term M and a set S of terms, the function `CHECK` tells us whether the term M can be built using the extension of S computed by the function `EXTEND`.

ACCEPTED MANUSCRIPT

The correctness of these algorithms will be proven separately.

We assume that terms are flattened so arguments of $\oplus$ cannot be headed with $\oplus$. In the functions defined below, each time we check if a term belongs to a set of terms, we consider equality modulo AC: $t \in_{AC} S$ means that a term AC-equivalent to t is in S.

Algorithm 1 Building contexts using terms in S

```
1: function BUILD(N, S)
2:     let P = {q_i ∈ Pos(N) | N|_{q_i} ∈_AC S and ∀q < q_i, N|_q ∉_AC S}   ▷ q_i highest s.t. N|_{q_i} ∈_AC S.
3:         N' = N[□]_{q_1} ... [□]_{q_k}, where {q_1, ..., q_k} = P
4:     in
5:     if N' does not contain private names then true
6:     else false
7:     end if
8: end function
```

BUILD takes as input a ground term N in normal form and a finite set S of ground terms in normal form, and checks in a top-down manner, whether there are terms in S that are subterms (modulo AC) of N. For this, BUILD uses P, the set of all positions p in N such that $N|_p =_{AC} s$, for some term $s \in S$. Those subterms are cut out of N, resulting in a term $N' = N[\Box]_{q_1} \dots [\Box]_{q_k}$ for $q_i \in P$. If there are no private names in N' it follows that N can be constructed from terms in $[S]_{AC}$, function symbols and public names, that is, $N =_{AC} C[s_1, \dots, s_k]$, with $s_j \in_{AC} S$ and a context C such that $names(C) \cap \tilde{n} = \emptyset$; otherwise, N cannot be constructed.

Algorithm 2 Extending the set S with sums

```
1: function EXTEND(M, S)
2:     let P_⊕ = [p_1, ..., p_k] be the list of positions in M headed by ⊕, in decreasing
3:                                  lexicographical order                ▷ Inner terms are listed first.
4:         T = {m_ij | ∃p_i ∈ P_⊕ s.t. M|_{p_i} = m_i1 ⊕ ... ⊕ m_ik_i}   ▷ Arguments of sums in M.
5:         S_0 = S ∪ {m_ij | m_ij ∈ T and BUILD(m_ij, S)}
6:         for 1 ≤ i ≤ k:
7:         S_i = if DIOPHANTINE(M|_{p_i}, S_{i-1})
8:                 then S_{i-1} ∪ {M|_{p_i}} ∪ {m_ij | m_ij ∈ T and BUILD(m_ij, S_{i-1} ∪ {M|_{p_i}})}
9:                 else S_{i-1}
10:    in S_k
11: end function
```

EXTEND(M, S) deals with the subterms of M headed by $\oplus$, in a bottom-up manner (see Algorithm 2). It extends the set S incrementally: if there are k subterms headed by $\oplus$ in M, it builds sets $S_0, \dots, S_k$ by checking each sum (using DIOPHANTINE) in inner-outer order. If a subterm $M|_{p_i}$ can be written as a linear combination of terms in S_{i-1}, then it is added to the set S_i and so the next term headed with $\oplus$ can use it; otherwise, it will not be added and $S_i = S_{i-1}$. To summarise, S_k can be described as

$$S_k = S \cup \left\{ \begin{array}{l} \text{linear combinations of } S^{AG}\text{-constructible summands that are} \\ \text{subterms of } M \text{ rooted by } \oplus \text{ or are summands of } M. \end{array} \right\} \quad (1)$$

ACCEPTED MANUSCRIPT

Algorithm 3 Reduction to linear Diophantine equations

1: **function** DIOPHANTINE(M, S)
2: **INPUT:** a term M headed by the operator $\oplus$ and the set S of terms built by EXTEND.
3: Note that if M is headed with $\oplus$ then

$$M = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r\,,\ \alpha_j \in \mathbb{N} \tag{2}$$

where m_j is not headed with $\oplus$ and $\alpha_j m_j$ denotes $\underbrace{m_j \oplus \ldots \oplus m_j}_{\alpha_j - times}$.

4: Let ▷ See Remark 2

$$\mathcal{S}_M = \begin{cases} (\beta_1\gamma_{1_1} \oplus \beta_2\gamma_{1_2} \oplus \ldots \oplus \beta_q\gamma_{1_q}) = \alpha_1 \\ \vdots \\ (\beta_1\gamma_{r_1} \oplus \beta_2\gamma_{r_2} \oplus \ldots \oplus \beta_q\gamma_{r_q}) = \alpha_r \\ (\beta_1\delta_{1_1} \oplus \beta_2\delta_{2_1} \oplus \ldots \oplus \beta_q\delta_{q_1}) = \mathbf{0} \\ \vdots \\ (\beta_1\delta_{1_k} \oplus \beta_2\delta_{2_k} \oplus \ldots \oplus \beta_q\delta_{q_k}) = \mathbf{0} \end{cases}$$

▷ $\mathcal{S}_M$ is a SLDE and over $\mathbb{Z}$, over the unknowns $\beta_1, \ldots, \beta_q$, which can be solved in polynomial time [26, 40].
5: **if** there is a solution for $\mathcal{S}_M$ **then** *True*
6: **else** *False*.
7: **end if**
8: **end function**

DIOPHANTINE is called by EXTEND to check whether $M|_{p_i}$ can be obtained as a linear combination of the terms in S_{i-1}. In general DIOPHANTINE(M, S), where M is a term headed by $\oplus$ and S is a set of terms, checks whether there are $\beta_1, \ldots, \beta_q \in \mathbb{N}$ such that

$$\beta_1 T_1 \oplus \ldots \oplus \beta_q T_q =_{AG} M = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r \tag{3}$$

for $T_1, \ldots, T_q \in S$ and known coefficients $\alpha_1, \ldots, \alpha_r$. This AG-equality is only possible when

$$T_i =_{AC} \gamma_{1i} m_1 \oplus \ldots \oplus \gamma_{ri} m_r \oplus \underbrace{(\delta_{i_1} u_{i_1} \oplus \ldots \oplus \delta_{i_k} u_{i_k})}_{\mathbf{u_i}},$$

for some u_{i_j} $(1 \le j \le k)$ which does not contain any m_i [6], for each i, $1 \le i \le q$. The coefficients $\gamma_{i_j}, \delta_i \in \mathbb{N}$ indicate the number of times a subterm occurs, and are computed from S and M using AC-matching. The role of $\mathbf{u_i}$ is the following: $\mathbf{u_i}$ denotes possible subterms in T_i that will be eliminated after the normalisation, for there is an index j such that T_j contains $i(\mathbf{u_i})$ as a subterm. Suppose that : $\mathbf{u_1} = \delta_{1_1} u_{1_1} \oplus \ldots \oplus \delta_{1_k} u_{1_k} \quad \ldots \quad \mathbf{u_q} = \delta_{q_1} u_{q_1} \oplus \ldots \oplus \delta_{q_k} u_{q_k}$.

We can rewrite these identities, modulo AG, in order to have the same u_{i_j} in every identity, by associating the coefficient $\mathbf{0}$ to the u_{i_j} that does not appear in $\mathbf{u}_l$, for instance, if $\mathbf{u}_1 = a + b + c$

[6] Note that $\mathbf{u_i}$ could be empty, that is, k could be 0.

ACCEPTED MANUSCRIPT

and $\mathbf{u}_2 = b + d$ then we can rewrite them as $u'_1 = a + b + c + \mathbf{0}d$ and $u'_2 = \mathbf{0}a + b + \mathbf{0}c + d$. Assuming that every $\mathbf{u}_i$ has been rewritten in this way, we obtain:

$$\begin{aligned} \mathbf{u'_1} &= \delta_{1_1} u_{1_1} \oplus \delta_{1_2} u_{1_2} \oplus \ldots \oplus \delta_{1_k} u_{1_k} \\ &\vdots \\ \mathbf{u'_q} &= \delta_{q_1} u_{1_1} \oplus \delta_{q_2} u_{1_2} \oplus \ldots \oplus \delta_{q_k} u_{1_k} \end{aligned} \tag{4}$$

and δ_{i_j} may be $\mathbf{0}$, for $1 \leq i \leq q$ and $1 \leq j \leq k$.

Remark 2. Note that

$$\beta_1 T_1 \oplus \ldots \oplus \beta_q T_q =_{AG} \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r$$

if and only if

$$\begin{aligned} &\beta_1(\gamma_{1_1} m_1 \oplus \ldots \oplus \gamma_{r_1} m_r \oplus \mathbf{u'_1}) \oplus \\ &\beta_2(\gamma_{1_2} m_1 \oplus \ldots \oplus \gamma_{r_2} m_r \oplus \mathbf{u'_2}) \oplus \\ &\qquad\qquad \vdots \\ &\beta_q(\gamma_{1_q} m_1 \oplus \ldots \oplus \gamma_{r_q} m_r \oplus \mathbf{u'_q}) = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r \oplus \mathbf{0}u_{1_1} \oplus \ldots \oplus \mathbf{0}u_{1_k} \end{aligned} \tag{5}$$

if and only if (after reorganising the coefficients and by (4))

$$\begin{aligned} &(\beta_1\gamma_{1_1} \oplus \beta_2\gamma_{1_2} \oplus \ldots \oplus \beta_q\gamma_{1_q}) m_1 \oplus \\ &(\beta_1\gamma_{2_1} \oplus \beta_2\gamma_{2_2} \oplus \ldots \oplus \beta_q\gamma_{2_q}) m_2 \oplus \\ &\qquad\qquad \vdots \\ &(\beta_1\gamma_{r_1} \oplus \beta_2\gamma_{r_2} \oplus \ldots \oplus \beta_q\gamma_{r_q}) m_r \oplus \\ &(\beta_1\delta_{1_1} \oplus \beta_2\delta_{2_1} \oplus \ldots \oplus \beta_q\delta_{q_1}) u_{1_1} \oplus \\ &\qquad\qquad \vdots \\ &(\beta_1\delta_{1_k} \oplus \beta_2\delta_{2_k} \oplus \ldots \oplus \beta_q\delta_{q_k}) u_{1_k} = \alpha_1 m_1 \oplus \ldots \oplus \alpha_r m_r \oplus \mathbf{0}u_{1_1} \oplus \ldots \oplus \mathbf{0}u_{1_k} \end{aligned} \tag{6}$$

if and only if,

$$S_M = \begin{cases} (\beta_1\gamma_{1_1} \oplus \beta_2\gamma_{1_2} \oplus \ldots \oplus \beta_q\gamma_{1_q}) = \alpha_1 \\ \qquad\qquad \vdots \\ (\beta_1\gamma_{r_1} \oplus \beta_2\gamma_{r_2} \oplus \ldots \oplus \beta_q\gamma_{r_q}) = \alpha_r \\ (\beta_1\delta_{1_1} \oplus \beta_2\delta_{2_1} \oplus \ldots \oplus \beta_q\delta_{q_1}) = \mathbf{0} \\ \qquad\qquad \vdots \\ (\beta_1\delta_{1_k} \oplus \beta_2\delta_{2_k} \oplus \ldots \oplus \beta_q\delta_{q_k}) = \mathbf{0} \end{cases}$$

Remark 3. When dealing with equational theories with inverses, the coefficients in equation 6 can be interpreted as integers rather than natural numbers: If there exists an index j such that $m_j = i(m'_j)$ and m'_j is not headed with i, that is, $\alpha_j m_j = \alpha_j(i(m'_j))$, then we interpret it as $(-\alpha_j)m'_j$. Therefore, we can assume $\alpha_j \in \mathbb{Z}$, for all j. Similarly, the unknowns $\beta_1, \ldots, \beta_q$ will range over $\mathbb{Z}$ and the coefficients $\gamma_{j_i}, \delta_{j_i} \in \mathbb{Z}$, for all i and j.

Before presenting the correctness proof for the algorithm, we give examples. The first one is simply illustrating the use of AG-equality to deal with **I**-locally stable theories.

ACCEPTED MANUSCRIPT

Example 5. Consider the theory $E = ACUI_+$, which we prove to be **I**-locally stable in Section 6.1. Given a set $\Gamma = \{a + i(b), b + b\}$, assume that $\tilde{n} = \{a, b\}$ and $M = f(a + b)$, for some $f \in \Sigma$. We want to check whether M can be obtained from the saturation set:

$$sat(\Gamma) = \{a + i(b), b + b, a + b, a + a, i(a) + b, i(b) + i(b), i(a) + i(b), i(a) + i(a)\}.$$

We use the function EXTEND to extend the set $sat(\Gamma)$ with the sums of M that can be constructed from $sat(\Gamma)$. Let $P_\oplus = \{1\}$ be the position of M headed with +. Initially, $T = \{a, b\}$ and $S_0 = sat(\Gamma) \cup \{m \in T \mid \texttt{BUILD}(m, S_0)\} = sat(\Gamma)$. Notice that $\texttt{DIOPHANTINE}(a + b, S_0) = true$, since $a + b \in sat(\Gamma)$ and $S_1 = sat(\Gamma)$. Therefore, $\texttt{EXTEND}(M, sat(\Gamma)))=sat(\Gamma)$.

Finally, $\texttt{CHECK}(M, sat(\Gamma)) = \texttt{BUILD}(M, \texttt{EXTEND}(M, sat(\Gamma))) = \texttt{BUILD}(M, sat(\Gamma)) = true$ since $M' = f[\Box]_1$ does not contain private symbols.

Example 6. To illustrate the algorithm, consider an **I**-locally stable theory E, whose signature is $\Sigma_E = \{+, i, 0\}$ and $\Sigma = \Sigma_E \cup \{f\}$, where f is a binary public function symbol (not AC),+ is a binary and AC function symbol, i is the inverse operator w.r.t + and 0 is the neutral element.

Suppose given $\Gamma = \{a + b + i(k), c + 2i(k), d + i(a) + i(b), i(d)\}$, $\tilde{n} = \{a, b, c\}$ and $M = a + b + c + f(i(a) + i(b))$ all ground and in normal form.

The set $sat(\Gamma)$ (computed according to the method given in Section 6.1 and organised in decreasing order) is:

$$\begin{aligned} sat(\Gamma) = {} & \{2i(a) + 2i(b) + c, 2a + 2b + i(c), i(a) + i(b) + c + i(k), a + b + i(c) + k, i(a) + i(b) + c\} \\ & \cup \{d + i(a) + i(b), i(a) + i(b) + k, a + b + i(c), a + b + i(k), i(d) + a + b\} \\ & \cup \{c + 2i(k), i(c) + 2k, i(a) + i(b), i(k) + d, c + i(k), i(c) + k, a + b\} \cup \{i(d), i(k), i(c), k, d, c\} \end{aligned}$$

The call $\texttt{EXTEND}(M, sat(\Gamma)) = \texttt{EXTEND}(a + b + c + f(i(a) + i(b)), sat(\Gamma))$ computes

- $P_\oplus = \{41, \varepsilon\}$, i.e., the set of positions in M headed with +.
- $T = \{a, b, c, i(a), i(b), f(i(a) + i(b))\}$
- $S_0 = sat(\Gamma) \cup \{m \in T \mid \texttt{BUILD}(m, sat(\Gamma))\} = sat(\Gamma) \cup \{c\}$
- $\texttt{DIOPHANTINE}(i(a) + i(b), S_0) = true$ since $i(a) + i(b) \in S_0$ and S_0 is extended to

$$\begin{aligned} S_1 &= S_0 \cup \{i(a) + i(b)\} \cup \{m \in T \mid \texttt{BUILD}(m, S_0 \cup \{i(a) + i(b)\})\} \\ S_1 &= S_0 \cup \{i(a) + i(b), f(i(a) + i(b))\}. \end{aligned}$$

- $\texttt{DIOPHANTINE}(a+b+c+f(i(a)+i(b), S_1) = true$ since $a+b, c, f(i(a)+i(b)) \in S_1$, therefore $S_2 = S_1 \cup \{M\}$.

Therefore, $\texttt{CHECK}(M, sat(\Gamma)) = \texttt{BUILD}(M, \texttt{EXTEND}(M, sat(\Gamma))) = \texttt{BUILD}(M, S_2) = true$, because in BUILD one has $M' = M[\Box]_\varepsilon$, which does not contain private names.

We now prove the correctness of the algorithms.

Lemma 10 (Correctness of BUILD)**.** *Given a ground term M in normal form and a finite set S of terms in normal form,* $\texttt{BUILD}(M, S)$ *correctly checks whether M is $(S')^\emptyset$-constructible, for $S' = [S]_{AC}$.*

ACCEPTED MANUSCRIPT

Proof. Let M be a ground term in normal form and S be a finite set of ground terms in normal form.

1. Suppose that $\texttt{BUILD}(M, S) = true$.

   There exists a set P of positions in M (as defined in BUILD) such that $M' = M[\Box]_{q_1} \dots [\Box]_{q_k}$, for $q_1, \dots, q_k \in P$ and M' does not contain private names as subterms. Therefore, M' is a context containing only function symbols from the signature and public names. Notice that the holes of M' will be filled with terms in S, and the membership is modulo AC, therefore M is clearly $(S')^{\emptyset}$-constructible.

2. Suppose that $\texttt{BUILD}(M, S) = false$. That is, $M' = M[\Box]_{q_1} \dots [\Box]_{q_k}$, for $q_1, \dots, q_k \in P$ and the context M' does contain some private name, say A, as subterm. Notice that, if there was another combination of positions in P, say, $p_1, \dots, p_t$, such that $M'' = M[\Box]_{p_1} \dots [\Box]_{p_t}$ and M'' is a context that does not contain private names, then there would exist some position $p_j \in P$ such that $p_j < q_i$ for some $q_i \in P$ and $M|_{p_j} \in_{AC} S$ and $A = (M_{p_j})|_q$, for some q, that is, A is a subterm of $M|_{p_j}$. But then, this would contradict the definition of P which says that for all $q < q_i$, $M|_q \notin_{AC} S$. Therefore, M cannot be written as a context whose holes are terms from S, that is, M is not $(S')^{\emptyset}$-constructible.

□

Lemma 11 (Correctness of EXTEND)**.** *Let S_k be the set computed by the function* $\texttt{EXTEND}(M, S)$ *and $S' = [S_k]_{AC}$. M is S^{AG}-constructible iff M is $(S')^{\emptyset}$-constructible.*

Proof.

$$M \text{ is } (S')^{\emptyset}\text{-constructible} \Leftrightarrow \exists C : M == C[T_1, \dots, T_i, \dots, T_n], T_i \in_{AC} S_k, i = 1, \dots, n$$
$$\Leftrightarrow_{(*)} \exists C : M =_{AG} C[T_1, \dots, \oplus(C_{i_1}[T'_{11}, \dots, T'_{1s_1}], \dots, C_{i_{n_i}}[T'_{n_i1}, \dots, T'_{n_is_{n_i}}]), \dots, T_n], T'_j \in S$$
$$\Leftrightarrow \exists C' : M =_{AG} C'[T'_1, \dots, T'_{11}, \dots, T_{n_i1}, \dots, T'_n], \text{ for } T'_l \in S \Leftrightarrow M \text{ is } S^{AG}\text{-constructible.}$$

(∗)In the algorithm EXTEND, the function DIOPHANTINE is used to build the set S_k such that

$$S_k = S \cup \left\{ \begin{array}{l} \text{linear combinations of } S^{AG}\text{-constructible summands that are subterms of } M \\ \text{rooted by } \oplus \text{ or are summands of } M. \end{array} \right\}$$

Therefore, either $T_i \in S$; or $T_i = \oplus(T_{i_1}, \dots, T_{i_{n_i}})$, T_{i_j} is S^{AG}-constructible and $M|_p = T_i$ for some position p. That is, $T_{i_j} =_{AG} C_{i_j}[T'_{j1}, \dots, T'_{js_j}]$, for $T'_{j_l} \in S$ and $j = 1, \dots, n_i$. Therefore, $T_i =_{AG} \oplus(C_{i_1}[T'_{11}, \dots, T'_{1s_1}], \dots, C_{i_{n_i}}[T'_{n_i1}, \dots, T'_{n_is_{n_i}}])$. □

Lemma 12 (Correctness of CHECK)**.** $\texttt{CHECK}(M, sat(\Gamma))$ *if, and only if, M is $sat(\Gamma)^{AG}$-constructible.*

Proof. On one hand, by the correctness of EXTEND (Lemma 11),

$$M \text{ is } sat(\Gamma)^{AG}\text{-constructible} \Leftrightarrow M \text{ is } (S')^{\emptyset}\text{-constructible, for } S' = [sat(\Gamma)_k]_{AC}$$

On the other hand, by the definition of CHECK,

$$\begin{aligned} \texttt{CHECK}(M, sat(\Gamma)) &\Leftrightarrow \texttt{BUILD}(M, \texttt{EXTEND}(M, sat(\Gamma))), \text{ by the correctness of BUILD,} \\ &\Leftrightarrow M \text{ is } (S')^{\emptyset}\text{-constructible, with } S' = [\texttt{EXTEND}(M, sat(\Gamma))]_{AC} \\ &\Leftrightarrow M \text{ is } (S')^{\emptyset}\text{-constructible, with } S' = [sat(\Gamma)_k]_{AC} \end{aligned}$$

□

ACCEPTED MANUSCRIPT

As a consequence, we obtain the correctness of the algorithm and the decidability of the IDP.

Theorem 13 (Correctness)**.** CHECK(M, $sat(\Gamma)$) *if, and only if,* $\Gamma \vdash M$.

Proof. By Lemmas 9 and 12: CHECK(M, $sat(\Gamma)$) iff M is $sat(\Gamma)^{AG}$-constructible iff $\Gamma \vdash M$. □

Corollary 14 (Polynomial Decidability)**.** *Let E be an* ***I****-locally stable theory. If* $\Gamma = \{M_1, \ldots, M_n\}$ *is a finite set of ground terms in normal form, ñ a set of private names and M a ground term in normal form, then the IDP, that is,* $\Gamma \vdash M$ *is decidable in polynomial time in* $|M|$ *and* $|sat(\Gamma)|$.

Proof. The result follows directly from Theorem 13. Notice that each step of the algorithm can be done in polynomial time in $|M|$ and $|sat(\Gamma)|$ because the number of terms added to the set sat by the function EXTEND is bounded by $|M|$ (only subterms of M that are constructible from $sat(\Gamma)$ are added). □

5.3. Algorithm CHECK *for* **N***-locally stable theories*

The algorithms provided in Section 5.2 can be adapted to solve the IDP for **N**-locally stable theories *without* inverses. Their correctness can be proved in the same way as in the previous section, thus obtaining Lemma 15, from which Theorem 6 follows.

The main difference is in the function DIOPHANTINE, which should now work with coefficients over $\mathbb{N}$ (natural numbers), that is, in Algorithm 3, the system of linear Diophantine equations will be solved over $\mathbb{N}$, which is an NP-complete problem [27].

The algorithm EXTEND should also be adapted to compute S_k via the new version of the function DIOPHANTINE with coefficients over $\mathbb{N}$.

Correctness of EXTEND (Lemma 11) can be obtained for **N**-locally stable theories as follows.

$$M \text{ is } (S')^{\emptyset}\text{-constructible} \Leftrightarrow \exists C : M == C[T_1, \ldots, T_i, \ldots, T_n], T_i \in_{AC} S_k, i = 1, \ldots, n$$
$$\Leftrightarrow \exists C : M =_{AC} C[T_1, \ldots, \oplus(C_{i_1}[T'_{11}, \ldots, T'_{1s_1}], \ldots, C_{i_{n_i}}[T'_{n_i 1}, \ldots, T'_{n_i s_{n_i}}]), \ldots, T_n], T'_j \in S$$

Similarly, one can obtain the correctness of CHECK for **N**-locally stable theories

$$\text{CHECK}(M, sat(\Gamma)) \Leftrightarrow M \text{ is } sat(\Gamma)^{AC}\text{-constructible} \Leftrightarrow M \text{ is } (S')^{\emptyset}\text{-constructible, for } S' = [S_k]_{AC}$$

Lemma 15. *Let E be a* ***N****-locally stable theory without inverses,* $\Gamma = \{M_1, \ldots, M_n\}$ *a finite set of ground messages in normal form, ñ a set of private names and M a ground term in normal form. Then the question of whether M is* $sat(\Gamma)^{AC}$*-constructible is decidable in non-deterministic polynomial time in* $|M|$ *and* $|sat(\Gamma)|$.

Proof. We proceed as in the case of **I**-locally stable theories, using the new versions of the algorithms BUILD, EXTEND, CHECK and DIOPHANTINE, however, since we do not have inverses, we restrict the matching problem to operate modulo associativity and commutativity only. Since in Algorithm 3 the system of linear Diophantine equations will be solved over $\mathbb{N}$ (naturals), we obtain a non-deterministic polynomial time complexity. □

There has been some efforts to design efficient procedures to find positive solutions for SLDE. When $\Sigma = \{+\}$, that is when the signature is reduced to one *AC* symbol, or possibly one *AC* symbol plus free constants, the problem reduces to combining the minimal positive solutions of linear Diophantine equations [12]. There are two main methods, by Huet [29] and by Clausen and Fortenbacher [17]. An extension of Fortenbacher's method to solve directly systems of linear Diophantine equations is presented in [12].

ACCEPTED MANUSCRIPT

6. Applications

In this section we show that the usual AC-equational theories used in cryptographic protocols can be classified either as **N**- or **I**-locally stable theories. The IDP for theories described in the following subsections have been studied previously, each one using a different approach. The aim of this section is to show that the method proposed in this paper is general enough to deal with all of them.

6.1. Abelian Groups

This subsection is concerned with proving that the theory of Abelian Groups ($ACUI_+$) is **I**-locally stable. The challenge is to find a finite saturated set of terms, given a finite Γ and $\tilde{n}$.

Example 2 specifies the equational theory E_{AG} and the corresponding rewriting system for Abelian Groups, with the signature $\Sigma_{AG} = \{+, 0, i\}$, where + is a binary associative-commutative function symbol, i is a unary function symbol, the *inverse*, and 0 is a constant, the *neutral element*.

Proposition 16. *The TRS $\mathcal{R}_{AG}$ defined in Example 2 is AC-convergent.*

Proof. We have checked AC-termination and AC-confluence using CiME3 [19]. Termination can be verified via the lexicographic path order $>_{lpo}$ on $T(\Sigma, X \cup \mathcal{N})$ induced by the order $i > + > 0$ on the symbols from Σ. For the confluence, one has to check that all the critical pairs are joinable (modulo AC). □

Since the signature Σ_{AG} of Abelian Groups contains the AC-function symbol +, to define a set *sat* for this equational theory, one has to define an adequate notion of subterms st_{AG} modulo associativity and commutativity of +. For this purpose, the notions of *atoms* (Definition 13), *subterms* and *linear combinations of subterms* (SS_+) will be defined and will be part of the construction of st_{AG} :

Definition 19 ($S_{AG}(T)$)**.** *Let t be a term in normal form. $S_{AG}(t)$ is the smallest set such that $t \in S_{AG}(t)$;*

- *if $i(u) \in S_{AG}(t)$ then $u \in S_{AG}(t)$;*
- *if $u = u_1 + u_2 + \ldots + u_n \in S_{AG}(t)$ then $atoms(u) \subset S_{AG}(t)$.*

This notion can be extended to a set T of subterms in the usual way: $S_{AG}(T) := \bigcup_{t \in T} S_{AG}(t)$.

Given a set T of ground terms in normal form, the following set stands for the set of (natural) linear combinations of the subterms of T:

Definition 20 ($SS_+(T)$)**.** *Let T be a finite set of ground terms in normal form, define $SS_+(T)$ as the set $SS_+(T) := \left\{ (\sum_{s \in M} \alpha_s s) \downarrow \mid M \subseteq S_{AG}(T), \alpha_s \in \mathbb{N} \right\}$.*

Given a set T of ground terms in normal form, the set $st_{AG}(T)$ of subterms defined below takes into account the (natural) linear combinations of $SS_+(T)$ that effectively occur in T.

Definition 21 ($st_{AG}(T)$)**.** *Let T be a set of ground terms in normal form, define $st_{AG}(T)$ as*

$$st_{AG}(T) := \{M \in SS_+(T) \mid M =_{AC} t_1|_p, \text{ for a term } t_1 \in S_{AG}(T) \text{ and some } p \in \mathcal{P}os(t_1)\} \cup S_{AG}(T)$$

ACCEPTED MANUSCRIPT

We have to show that for every finite set $\Gamma = \{M_1, \ldots, M_k\}$ of ground terms in normal form, and a set $\tilde{n}$, there exists a finite and computable set $sat(\Gamma)$ satisfying the conditions 1-5 of Definition 12. The following example gives us some ideas for the construction of $sat(\Gamma)$.

Example 7. Let $\Gamma = \{a + 2b + c + d, i(b) + m + n, 2i(c) + i(m) + g, i(n) + 2d\}$ be a set of messages built from $\Sigma_{AG} \cup \mathcal{N}$.

Let $C[\_] := \_ + \_$ be an E_{AG}-context and $T_1 = a + 2b + c + d, T_2 = i(b) + m + n, T_3 = 2i(c) + i(m) + g \in sum_+(sat(\Gamma), \tilde{n})$. Taking $S_i = T_i \in sum_+(sat(\Gamma), \tilde{n}), i = 1, 2, 3$ below:

$$C[S_1, S_2] = (a + 2b + c + d) + (i(b) + m + n) \xrightarrow{h} a + b + 0 + c + d + m + n = M$$

$$C[S_1, S_3] = (a + 2b + c + d) + (2i(c) + i(m) + g) \xrightarrow{h} a + 2b + d + 0 + i(c) + i(m) + g = N$$

both reductions via rule $x + i(x) \to 0$.

The definition of $sat(\Gamma)$ has to guarantee that $M \xrightarrow{*} M' =_{AC} C'[S'_1, \ldots, S'_k]$ for $S'_1, \ldots, S'_k \in sum_+(sat(\Gamma), \tilde{n})$ and $N \xrightarrow{*} N' =_{AC} C''[S''_1, \ldots, S''_r]$ for $S''_1, \ldots, S''_r \in sum_+(sat(\Gamma), \tilde{n})$.

Adding $M\downarrow$ and $N\downarrow$ in $sat(\Gamma)$ helps to overcome this situation.

The problem is: the iteration of the reasoning above generates a linear combination of terms $(\alpha_1 t_1 + \alpha_2 t_2 + \ldots + \alpha_n t_n)\downarrow$ for $\alpha_i \in \mathbb{N}$ which will be added in $sat(\Gamma)$. If the group under consideration is not finite, this linear combination seems to generate an infinite number of terms that will be added in $sat(\Gamma)$, which makes it impossible to show that the equational theory of Abelian Groups is **I**-locally stable. However, there is a way to bound these combinations: we will give some intuition by analysing some cases.

Below, we consider a simple example in which only one atom can be part of a rewriting reduction using rules for neutral and inverses.

Example 8. Consider the set $\Gamma = \{\underbrace{a + b + c}_{t_1}, \underbrace{a + r}_{t_2}, \underbrace{a + s}_{t_3}\}$. For the construction of the saturation set, we will include $\Gamma \cup \{i(\Gamma)\downarrow\}$ in $sat(\Gamma)$.

Note that $i(\Gamma)\downarrow = \{\underbrace{i(a) + i(b) + i(c)}_{t'_1}, \underbrace{i(a) + i(r)}_{t'_2}, \underbrace{i(a) + i(s)}_{t'_3}\}$.

Starting with t_1, the following terms will be added in $sat(\Gamma)$:

$$t_1 + t'_2 \xrightarrow{h} 0 + b + c + i(r) \xrightarrow{*} b + c + i(r) = (\mathbf{t_1} + \mathbf{t'_2})\downarrow$$
$$t_1 + t'_3 \xrightarrow{h} 0 + b + c + i(s) \xrightarrow{*} b + c + i(s) = (\mathbf{t_1} + \mathbf{t'_3})\downarrow$$
$$2t_1 + t'_2 \xrightarrow{*} (t_1 + (t_1 + t'_2))\downarrow = \mathbf{t_1} + (\mathbf{t_1} + \mathbf{t'_2})\downarrow$$
$$2t_1 + t'_3 \xrightarrow{*} (t_1 + (t_1 + t'_3))\downarrow = \mathbf{t_1} + (\mathbf{t_1} + \mathbf{t'_3})\downarrow$$

$$2t_1 + 2t'_2 \xrightarrow{*} 2(\mathbf{t_1} + \mathbf{t'_2})\downarrow$$
$$2t_1 + 2t'_3 \xrightarrow{*} 2(\mathbf{t_1} + \mathbf{t'_3})\downarrow$$
$$2t_1 + t'_2 + t'_3 \xrightarrow{*} (\mathbf{t_1} + \mathbf{t'_2})\downarrow + (\mathbf{t_1} + \mathbf{t'_3})\downarrow$$

Notice the following facts:

- the atom a can be eliminated via rewriting using rules $x + i(x) \to 0$ and $x + 0 \to x$, if one combines the terms in $\Gamma \cup \{i(\Gamma)\downarrow\}$;
- The coefficient of t_1 goes up to 2 which is the sum of occurrences of $i(a)$ in t'_2 and t'_3.
- If the terms $(t_1 + t'_2)\downarrow$ and $(t_1 + t'_3)\downarrow$ are added in $sat(\Gamma)$, the linear combinations of t_1, t'_2 and t'_3 considered above can be seen as E_{AG}-contexts whose holes are terms from $sat(\Gamma)$.
- It is easy to check that linear combinations whose coefficients are greater than 2 can be seen as multiples of one of the terms above.

ACCEPTED MANUSCRIPT

The same reasoning has to be repeated when starting with terms t_2 or t_3, new combinations may appear, however there will be a finite number of combinations.

Example 9. Consider $\Gamma = \{\underbrace{a+b+c}_{t_1}, \underbrace{a+r}_{t_2}, \underbrace{a+s}_{t_3}, \underbrace{b+m}_{t_4}, \underbrace{b+q}_{t_5}\}$ and $i(\Gamma) \downarrow = \{\underbrace{i(a)+i(b)+i(c)}_{t'_1}, \underbrace{i(a)+i(r)}_{t'_2}, \underbrace{i(a)+i(s)}_{t'_3}, \underbrace{i(b)+i(m)}_{t'_4}, \underbrace{i(b)+i(q)}_{t'_5}\}$.

Repeating the previous reasoning, starting with t_1 we add in $sat(\Gamma)$ the linear combinations for the possibilities of eliminating the atom a,

$$\begin{array}{ll} \mathbf{t_1} + \mathbf{t'_2} \xrightarrow{*} b + c + i(r) & \mathbf{t_1} + \mathbf{t'_3} \xrightarrow{*} b + c + i(s) \\ 2t_1 + t'_2 \xrightarrow{*} a + 2b + 2c + i(r) = \mathbf{t_1} + (\mathbf{t_1} + \mathbf{t'_2}) \downarrow & 2t_1 + t'_3 \xrightarrow{*} \mathbf{t_1} + (\mathbf{t_1} + \mathbf{t'_3}) \downarrow \\ 2t_1 + 2t'_2 \xrightarrow{*} 2b + 2c + 2i(r) = 2(\mathbf{t_1} + \mathbf{t'_2}) \downarrow & 2t_1 + 2t'_3 \xrightarrow{*} 2(\mathbf{t_1} + \mathbf{t'_3}) \downarrow \\ 2t_1 + t'_2 + t'_3 \xrightarrow{*} 2b + 2c + i(r) + i(s) & \end{array} \tag{7}$$

We repeat the reasoning for obtaining the combinations for eliminating atom b.

$$\begin{array}{ll} \mathbf{t_1} + \mathbf{t'_4} \xrightarrow{*} a + c + i(m) & \mathbf{t_1} + \mathbf{t'_5} \xrightarrow{*} a + c + i(q) \\ 2t_1 + t'_4 \xrightarrow{*} t_1 + (t_1 + t'_4) \downarrow & 2t_1 + 2t'_5 \xrightarrow{*} 2(t_1 + t'_5) \downarrow \\ 2t_1 + 2t'_4 \xrightarrow{*} 2(t_1 + t'_4) & 2t_1 + t'_4 + t'_5 \xrightarrow{*} (t_1 + t'_4) \downarrow + (t_1 + t'_5) \downarrow \\ 2t_1 + t'_5 \xrightarrow{*} t_1 + (t_1 + t'_5) \downarrow & \end{array} \tag{8}$$

We combine the terms obtained in (7) and (8), obtaining the following general term:

$$(\beta_1 t_1 + \beta_2 t'_2 + \beta_3 t'_3 + \beta_4 t'_4 + \beta_5 t'_5) \downarrow$$

whose coefficients satisfy the following conditions:

1. $1 \leq \beta_1 \leq lcm(\mathbf{m_a}, \mathbf{m_b})$ (we have to make sure that both atoms will be analysed fully)
   For eliminating a: $0 \leq \beta_1 \leq \frac{lcm(\alpha_{1a}, \sum_{j=2}^{5} \alpha'_{ja}, \alpha'_{2a}, \alpha'_{3a}, \alpha'_{4a})}{\alpha_{1a}} = \mathbf{m_a}$.
   For eliminating b: $0 \leq \beta_1 \leq \frac{lcm(\alpha_{1b}, \sum_{j=2}^{5} \alpha'_{jb}, \alpha'_{2b}, \alpha'_{3b}, \alpha'_{4b})}{\alpha_{1b}} = \mathbf{m_b}$.
   The coefficients $\alpha'_{ja} = |t'_j|_{i(a)}$, for $j = 1, \ldots, 5$ (α'_{jb} is similarly defined for atom b).
2. $1 \leq \beta_2 \alpha_{2_a} + \ldots + \beta_5 \alpha_{5_a} \leq \beta_1 \alpha_{1_a}$, where $\alpha_{1_a} = |t_1|_a$ and $\alpha'_{j_a} = |t'_j|_{i(a)}$, for $2 \leq j \leq 5$.
3. $1 \leq \beta_2 \alpha_{2_b} + \ldots + \beta_5 \alpha_{5_b} \leq \beta_1 \alpha_{1_b}$, where $\alpha_{1_b} = |t_1|_b$ and $\alpha'_{j_b} = |t'_j|_{i(b)}$, for $2 \leq j \leq 5$.

We have to proceed similarly starting with terms $t_2, t_3, \ldots, t_5$ and adjust the coefficients, taking the maximum, in order to satisfy all the combinations.

These examples suggest a general technique to bound the coefficients of the linear combinations added in $sat(\Gamma)$, the idea is to build the "subspace generated " by the finite set of atoms occurring in Γ.

ACCEPTED MANUSCRIPT

6.1.1. A bound for linear combinations in Abelian Groups

Let $\mathcal{G} = (G, +, 0)$ be an Abelian Group. Consider the following encoding, for all $x \in G$:

$$i(x) = -(x) \qquad \underbrace{x + x + \ldots + x}_{n\text{–times}} = n \cdot x \qquad n.(i(x)) = (-n) \cdot x$$

Using this encoding for multiplicity of elements of G, we obtain a notion of *scalar product*, and therefore, we can see $(G, +, \cdot, 0)$ as a module V, over $\mathbb{Z}$. A well-known result is that every Abelian Group is a module over $\mathbb{Z}$. A module is a generalisation of vector space, when the scalars are elements of a ring.

The *vector subspace of V generated by a subset A* of V (denoted by $S(A)$) is, by definition, the set of all linear combinations of elements $v_1, \ldots, v_m$ in A: $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_m v_m$.

We want to show that, taking into account the theory of Abelian Groups, given a finite set Γ of ground terms in normal form, there exists a finite set X_Γ, such that $(S(\Gamma)\downarrow_{\mathcal{R}_{AG}})$ can be obtained directly by combining elements in X_Γ (i.e., the set of normal forms w.r.t. $\mathcal{R}_{AG}$ of linear combinations of terms in Γ can be built directly by combining elements in X_Γ).

Step 1. Let $t_1, \ldots, t_k$ be terms in normal form in Γ and $t'_1, \ldots, t'_k$ be terms in $i(\Gamma)\downarrow$ with $t'_j = i(t_j)\downarrow$, such that $a_1, \ldots, a_r$ are the only atoms in t_j or t'_j $(j = 1, \ldots, k)$ which can be eliminated via application of rules $i(x) + x \to 0$ and $x + 0 \to x$.

Suppose that for $j = 1, \ldots, k$ one has

$$\begin{aligned} t_j &= \alpha_{j_1} a_1 + \ldots + \alpha_{j_t} a_t + \alpha_{j_{t+1}} i(a_{t+1}) + \ldots + \alpha_{j_r} i(a_r) + b_j \\ t'_j &= \alpha_{j_1} i(a_1) + \ldots + \alpha_{j_t} i(a_t) + \alpha_{j_{t+1}} a_{t+1} + \ldots + \alpha_{j_r} a_r + b'_j \end{aligned} \tag{9}$$

where b_j (respect. b'_j) does not contain occurrences of a_p(respect. $i(a_p)$) for $j = 1, \ldots, k$ and $p = 1, \ldots, r$.

Step 2. Denote by T the set of all possible (normalised) linear combinations of the terms $t_1, \ldots, t'_k$

$$\begin{aligned} T &= (\gamma_1 t_1 + \ldots + \gamma_k t_k + \gamma'_1 t'_1 + \ldots + \gamma'_k t'_k)\downarrow = (\sum_{j=1}^{k} \gamma_j t_j + \sum_{j=1}^{k} \gamma'_j t'_j)\downarrow \\ &=_{AC} \left(\sum_{j=1}^{k} \gamma_j (\sum_{l=1}^{t} \alpha_{j_l} a_l + \sum_{l=t+1}^{r} \alpha_{j_l} i(a_l) + b_j) + \sum_{j=1}^{k} \gamma'_j (\sum_{l=1}^{t} \alpha_{j_l} i(a_l) + \sum_{l=t+1}^{r} \alpha_{j_l} a_l + b'_j) \right)\downarrow \\ &=_{AC} \left(\sum_{u=1}^{t} (\sum_{j=1}^{k} \gamma_j \alpha_{j_u}) a_u + \sum_{u=t+1}^{r} (\sum_{j=1}^{k} \gamma_j \alpha_{j_u}) i(a_u) + \sum_{u=1}^{t} (\sum_{j=1}^{k} \gamma'_j \alpha_{j_u}) i(a_u) + \sum_{u=t+1}^{r} (\sum_{j=1}^{k} \gamma'_j \alpha_{j_u}) a_u + B + B' \right)\downarrow \end{aligned} \tag{10}$$

for $B = \sum_{j=1}^{k} \gamma_j b_j$ and $B' = \sum_{j=1}^{k} \gamma'_j b'_j$ and whose coefficients γ_j, γ'_j range over $\mathbb{Z}$, $j = 1, \ldots, k$ and $k \in \mathbb{N}$.

Step 3. Define a bound M^* for $\gamma_1, \ldots, \gamma_k, \gamma'_1, \ldots, \gamma'_k$, which depends on the terms in Γ, taking into account the reasoning used in the previous examples, that is, each γ_j, γ'_j has to range over the multiple[7] of the coefficients a_l and $i(a_l)$ (and their sum) occurring in t_j and in t'_j, for

[7] We only put in the *lcm* from Equation 11 the coefficients that are different from zero.

ACCEPTED MANUSCRIPT

each $1 \leq l \leq r$:

$$0 \leq \gamma_j, \gamma'_j \leq \frac{lcm(\alpha_{j_u}, \sum_{h\neq j} \alpha^*_{h_u}, \sum_{h\neq j} \alpha'_{h_u}, \alpha'_{l_{1u}}, \ldots, \alpha'_{l_{su}}, \alpha^*_{l_{1u}}, \ldots, \alpha^*_{l_{su}})}{\alpha_{j_u}} := \frac{m_{j_u}}{\alpha_{j_u}} \quad (1 \leq u \leq t)$$
$$0 \leq \gamma_j, \gamma'_j \leq \frac{lcm(\alpha_{j_v}, \sum_{h\neq j} \alpha^*_{h_v}, \sum_{h\neq j} \alpha'_{h_v}, \alpha'_{l_{1v}}, \ldots, \alpha'_{l_{sv}}, \alpha^*_{l_{1v}}, \ldots, \alpha^*_{l_{sv}})}{\alpha_{j_v}} := \frac{m_{j_v}}{\alpha_{j_v}} \quad (t+1 \leq v \leq r) \tag{11}$$

for each $1 \leq j \leq k$, where $\alpha_{j_p} = |t_j|_{a_p}$ (resp. $\alpha_{j_p} = |t_j|_{i(a_p)}$), that is, the number of occurrences of atom a_p (resp. $i(a_p)$) in the term $|t_j|$, for $1 \leq p \leq t$ (resp. for $t+1 \leq p \leq r$) and $1 \leq j \leq k$. Similarly,

$$\alpha'_{j_p} = \begin{cases} |t'_j|_{i(a_p)}, & \text{if } 1 \leq p \leq t \\ |t'_j|_{a_p}, & \text{if } t+1 \leq p \leq r \end{cases} \qquad \alpha^*_{j_p} = \begin{cases} |t_j|_{i(a_p)}, & \text{if } 1 \leq p \leq t \\ |t_j|_{a_p}, & \text{if } t+1 \leq p \leq r \end{cases}$$

Also, $\{l_1, \ldots, l_s\} = \{1, \ldots, k\} - \{j\}$.

Therefore,

$$0 \leq \gamma_j, \gamma'_j \leq lcm(\frac{m_{1_1}}{\alpha_{1_1}}, \ldots, \frac{m_{k_1}}{\alpha_{k_1}}) = M_1, \quad \ldots, \quad 0 \leq \gamma_j, \gamma'_j \leq lcm(\frac{m_{1_r}}{\alpha_{1_r}}, \ldots, \frac{m_{k_r}}{\alpha_{k_r}}) = M_r$$

In order to satisfy all the inequalities above, we will take $M^* = lcm(M_1, \ldots, M_r)$, therefore, the coefficients γ_j, γ'_j satisfy: $0 \leq \gamma_j, \gamma'_j \leq M^*$ for all $j = 1, \ldots, k$.

Step 4. Define the set $X_{(\Gamma,M^*)}$ as:

$$X_{(\Gamma,M^*)} = \left\{ \left(\left(\sum_{i=1}^{k} \gamma_j t_j \right) + \left(\sum_{j=1}^{k} \gamma'_j t'_j \right) \right) \downarrow \;\middle|\; \begin{array}{l} 0 \leq \gamma_j, \gamma'_j \leq M^* \text{ and for each } 1 \leq u \leq r \\ 0 \leq \sum_{j=1}^{k} \gamma'_j \alpha'_{j_u} + \sum_{j=1}^{k} \gamma_j \alpha^*_{j_u} \leq \sum_{j=1}^{k} \gamma_j \alpha_{j_u} + \sum_{j=1}^{k} \gamma'_j \alpha^*_{j_u}. \text{ or} \\ 0 \leq \sum_{j=1}^{k} \gamma_j \alpha_{j_u} + \sum_{j=1}^{k} \gamma'_j \alpha^*_{j_u} \leq \sum_{j=1}^{k} \gamma'_j \alpha'_{j_u} + \sum_{j=1}^{k} \gamma_j \alpha^*_{j_u} \end{array} \right\}$$

The second (resp. third) condition says that the sum of the number of occurrences of $i(a_u)$ (resp. a_u) in t_j or t'_j is bounded by the number of occurrences of a_u (resp. $i(a_u)$) in t_j and t'_j. These conditions depend on whether the number of occurrences of $i(a_u)$ is smaller than the number of occurrences of a_u, in the terms, for each of the u's.

For each choice of the coefficients [8] α we get one term in $X_{(\Gamma,M^*)}$. Since each γ_j ranges from 0 to M^* and γ'_j is bounded by the second inequality in the definition of $X_{(\Gamma,M^*)}$, we can conclude that the set $X_{(\Gamma,M^*)}$ is finite.

The next result says that the normal form of a term $t \in S(\Gamma)$ is a linear combination of terms in $X_{(\Gamma,M^*)}$.

Proposition 17. *Let $\Gamma = \{t_1, \ldots, t_k\}$ be a finite set of ground terms in normal form, such that, the identities in (9) are satisfied, and let $S(\Gamma)$ be the set of finite linear combinations of the terms in Γ. If M^* is constructed as in Step 2 above, then for $t \in S(\Gamma)$*

$$t{\downarrow_{\mathcal{R}_{AG}}} = \left(\sum_{j=1}^{k} \delta_j t_j + \sum_{j=1}^{k} \delta'_j i(t_j) \right) {\downarrow_{\mathcal{R}_{AG}}} = \lambda_1 \mathbf{T_1} + \ldots + \lambda_r \mathbf{T_r} \tag{12}$$

[8] The coefficients α_{j_i} come from (9)

ACCEPTED MANUSCRIPT

for δ_j, δ'_j ranging over the naturals and $\mathbf{T_i} \in X_{(\Gamma,M^*)}$. That is, every linear combination of terms in Γ reduces to a linear combination of terms in $X_{(\Gamma,M^*)}$.

Proof. The proof relies on combinatorics and linear algebra results, we give below the main ideas of the proof.

Let $t \in S(\Gamma)$ be the linear combination

$$t = (\delta_1 t_1 + \ldots + \delta_k t_k) + (\delta'_1 t'_1 + \ldots + \delta'_k t'_k)$$

for some $\delta_j, \delta'_j \in \mathbb{N}$, $1 \leq j \leq k$. Suppose that for some index u, $1 \leq u \leq k$, $\delta_u > M^*$, assume w.l.o.g, that $u = 1$, that is, $\delta_1 > M^*$. By the Chinese Remainder Theorem, $\delta_1 = M^* q_1 + r_1$, for some $0 \leq r_1 < M^*$ and $q_1 \in \mathbb{N}$. Therefore,

$$\begin{aligned} t &= (M^* q_1 + r_1) t_1 + (\delta_2 t_2 + \ldots + \delta_k t_k) + (\delta'_1 t'_1 + \ldots + \delta'_k t'_k) \\ &=_{AC} \underbrace{(r_1 t_1 + \delta_2 t_2 + \ldots + \delta_k t_k)}_{t'} + (\sum_{j=1}^{k} \delta'_j t'_j) + M^* q_1 t_1 \end{aligned} \tag{13}$$

If there exist other indices with such a property, we repeat the reasoning. To ease the presentation, we will assume that u is the only index whose corresponding coefficient is $> M^*$. Therefore, the term obtained in (13), satisfies the first part of the definition of $X_{(\Gamma,M^*)}$, in Step 4.

Now, one has to check whether $t' \in X_{(\Gamma,M^*)}$:

a) if $0 \leq \sum_{j=1}^{k} \delta'_j \alpha_{j_i} + \sum_{j=1}^{k} \delta'_j \alpha^*_{j_i} \leq r_1 \alpha_{1_i} + \sum_{j=2}^{k} \delta_j \alpha_{j_i} + \sum_{j=1}^{k} \delta'_j \alpha^*_{j_i}$, for each $i = 1, \ldots, r$, then

$$\begin{aligned} t &=_{AC} \underbrace{(r_1 t_1 + \delta_2 t_2 + \ldots + \delta_k t_k) + (\sum_{j=1}^{k} \delta'_j t'_j)}_{t'} + M^* q_1 t_1 \\ &\to^* \underbrace{\left(r_1 t_1 + \sum_{j=2}^{k} \delta_j t_j + \sum_{j=1}^{k} \delta'_j t'_j \right)\downarrow}_{\mathbf{T_1} \in X_{(\Gamma,M^*)}} + q_1 \underbrace{(M^* t_1)\downarrow}_{\mathbf{T_2} \in X_{(\Gamma,M^*)}} = \mathbf{T_1} + q_1 \mathbf{T_2} \end{aligned}$$

And the sum of occurrences of $i(a_j)$ is $\leq$ the sum of occurrences of a_j, therefore, there are only occurrences of a_j in $\mathbf{T_1}$. Hence, there is no reduction from $\mathbf{T_1} + \mathbf{T_2}$, otherwise, t_1 would contain occurrences of $i(a_l)$ and a_l with coefficients different from zero, contradicting the fact that t_1 is a term in normal form.

b) Suppose that for some i, for $1 \leq i \leq r$, $\sum_{j=1}^{k} \delta'_j \alpha_{j_i} + \sum_{j=1}^{k} \delta_j \alpha^*_{j_i} > r_1 \alpha_{1_i} + \sum_{j=2}^{k} \delta_j \alpha_{j_i} + \sum_{j=1}^{k} \delta'_j \alpha^*_{j_i}$. We assumed that the atoms that can be eliminated via the rules for AG are $a_1, \ldots, a_r$. Organising the terms in such a way that each one of the atoms occur in every term, that is, considering the possibility of null coefficients in the case that a specific atom does not occur in that term we obtain, the following term, for $i = 1$, $t_1 = \alpha_{1_1} a_1 + \alpha_{1_2} a_2 + \ldots + \alpha_{1_r} a_r + \alpha^*_{1_1} i(a_1) + \alpha^*_{1_2} i(a_2) + \ldots + \alpha^*_{1_r} i(a_r)$. Notice that, in the term above, if $\alpha_{1_1} \neq 0$ then the coefficient for $i(a_1)$ has to be null, otherwise, the term would not be in normal form.

ACCEPTED MANUSCRIPT

Assume, w.l.o.g, that the only [9]atom for which the condition 2 of the definition of $X_{(\Gamma,M^*)}$ does not follow is $i = 1$, then we have the following inequality:

$$\delta'_1\alpha_{1_1} + \delta'_2\alpha_{2_1} + \ldots + \delta'_k\alpha_{k_1} + \delta_1\alpha^*_{1_1} + \delta_2\alpha^*_{2_1} + \ldots + \delta_k\alpha^*_{k_1} + > r_1\alpha_{1_i} + \sum_{j=2}^{k}\delta_j\alpha_{j_i} + \sum_{j=1}^{k}\delta'_j\alpha^*_{j_i}$$

Consider the scenario in which $\alpha_{j_1} \neq 0$, for $1 \leq j \leq k$, then $\alpha^*_{j_1} = 0$, and $\delta'_1\alpha_{1_1} + \delta'_2\alpha_{2_1} + \ldots + \delta'_k\alpha_{k_1} > r_1\alpha_{1_i} + \sum_{j=2}^{k}\delta_j\alpha_{j_i}$ (In the case some $\alpha_{j_1} = 0$, one has $\alpha_{l_1} \neq 0$ for some $l \neq j$, the analysis in this case is similar.)

Let $\delta^*_1, \ldots, \delta^*_k$ maximal coefficients such that $0 \leq \delta^*_j \leq \delta'_j \leq M^*$, for $1 \leq j \leq k$

$$\delta^*_1\alpha_{1_1} + \delta^*_2\alpha_{2_1} + \ldots + \delta^*_k\alpha_{k_1} \leq r_1\alpha_{1_i} + \sum_{j=2}^{k}\delta_j\alpha_{j_i} \tag{14}$$

By the Chinese Remainder Theorem, it follows that $\delta'_j = \delta^*_j q_j + r_j$, for $0 \leq r_j < \delta^*_j$ and $1 \leq j \leq k$, where $q_j, q'_1 \in \mathbb{N}$, for $2 \leq j \leq k$. Therefore,

$$t =_{AC} \underbrace{(r_1t_1 + \delta_2t_2 + \ldots + \delta_kt_k) + (\sum_{j=1}^{k}\delta'_jt'_j)}_{t'} + M^*q_1t_1 =_{AC} \left(r_1t_1 + \sum_{j=2}^{k}\delta_jt_j + \sum_{j=1}^{k}(\delta^*_jq_j + r_j)t'_j\right) + M^*q_1t_1$$

$$=_{AC} \left(r_1t_1 + \sum_{j=2}^{k}\delta_jt_j + \sum_{j=1}^{k}(\delta^*_jq_j)t'_j\right) + \sum_{j=1}^{k}r_jt'_j + M^*q_1t_1$$

$$=_{AC} \left(r_1t_1 + \sum_{j=2}^{k}\delta_jt_j + \sum_{j=1}^{k}\delta^*_jt'_j\right) + \sum_{j=1}^{k}(\delta^*_j(q_j - 1))t'_j + \sum_{j=1}^{k}r_jt'_j + M^*q_1t_1$$

$$=_{AC} \left(r_1t_1 + \sum_{j=2}^{k}\delta_jt_j + \sum_{j=1}^{k}\delta^*_jt'_j\right) + \sum_{j=1}^{k}g_jt'_j + M^*q_1t_1, \text{ for } g_j = \delta^*_j(q_j - 1) + r_j$$

$$\overset{*}{\rightarrow}_{AC} \underbrace{\left(r_1t_1 + \sum_{j=2}^{k}\delta_jt_j + \sum_{j=1}^{k}\delta^*_jt'_j\right)\downarrow}_{\mathbf{T_1}\in X_{(\Gamma,M^*)}} + \underbrace{\sum_{j=1}^{k}g_jt'_j + M^*q_1t_1}_{R_1}$$

Notice condition 2 guarantees that all the occurrences of $i(a_1)$ were eliminated after the normalisation of t', there might exist occurrences of a_1.

From the identities in (14), it follows that $g_j \leq M^*$, for each $1 \leq j \leq k$.

b.1) If there is a reduction from R_1 then some atom can be eliminated via the rules for AG.

- if condition 2 is satisfied in R_1, for all the atoms a_j, for $1 \leq j \leq t$,

$$R_1 =_{AC} \left(M^*t_1 + \sum_{j=1}^{k}g_jt'_j\right) + (q_1 - 1)(M^*t_1) \overset{*}{\rightarrow}_{AC} \underbrace{\left(M^*t_1 + \sum_{j=1}^{k}g_jt'_j\right)\downarrow}_{\mathbf{T_2}\in X_{(\Gamma,M^*)}} + (q_1 - 1)\underbrace{(M^*t_1)}_{\mathbf{T_3}\in X_{(\Gamma,M^*)}}$$

[9]for the case in which other atoms do not satisfy the condition 2, the analysis is similar.

ACCEPTED MANUSCRIPT

We notice that all the occurrences of $i(a_j)$ that existed in $\mathbf{T_2}$ were eliminated, this follows from condition 2. Therefore, $t \overset{*}{\rightarrow}_{AC} \mathbf{T_1} + \mathbf{T_2} + (q_1 - 1)\mathbf{T_3}$ and $\mathbf{T_1} + \mathbf{T_2} + (q_1 - 1)\mathbf{T_3}$ is a normal form.

- If condition 2 is not satisfied, then we repeat the reasoning developed in b).

b.2) If there is no reduction from R_1, then $t \overset{*}{\rightarrow} \mathbf{T_1} + \underbrace{\sum_{j=1}^{k} g_j t'_j + M^* t_1}_{\mathbf{T_4} \in X_{(\Gamma, M^*)}} + q_1 \underbrace{t_1}_{\in X_{(\Gamma, M^*)}}$ and the term $\mathbf{T_1} + \mathbf{T_4} + q_1 t_1$ is irreducible.

The proof of the other cases can be done similarly. □

Definition 22. *Given a set $\Gamma = \{t_1, \ldots, t_n\}$, let K_Γ be the set of subterms of Γ given as*

$$K_\Gamma := \{t \in \Gamma : \exists\, a \in atoms(t)\ \exists\, t' \in \Gamma,\ t \neq t' \text{ such that } a \in atoms(t') \text{ or } i(a) \in atoms(t')\}$$

From Proposition 17 one can notice that it is enough to add in $sat(\Gamma)$ only the combinations of terms in K_Γ where the coefficients go up to the bound given in Conditions 1 and 2, both depend on the number of occurrences of each atom in K_Γ, all other combinations can be obtained from these ones.

Definition 23 ($sat(\Gamma)$ for E_{AG})**.** *For a given set $\Gamma = \{M_1, \ldots, M_k\}$ of ground terms in normal form and a set $\tilde{n}$ of private names, $sat(\Gamma)$ is the smallest set such that:*

1. *$M_1, \ldots, M_k \in sat(\Gamma)$ and $m \in sat(\Gamma)$ for every $m \in pn(\Gamma)$;*
2. *$M_1, \ldots, M_k \in sat(\Gamma)$ and $f(M_1, \ldots, M_k) \in st_{AG}(sat(\Gamma))$ then $f(M_1, \ldots, M_k) \in sat(\Gamma)$, $f \in \Sigma_{AG}$;*
3. *if $\{t'_1, \ldots, t'_n\} = K_\Gamma$ then $(\alpha_1 t'_1 + \alpha_2 t'_2 + \ldots + \alpha_n t'_n)\downarrow \in sat(\Gamma)$ where $\alpha_1, \ldots, \alpha_n$ are given by the Conditions 1 and 2 from Proposition 17.*
4. *if $M_j \in sat(\Gamma)$ then $i(M_j)\downarrow \in sat(\Gamma)$;*

Notice that some "sums" will be added in $sat(\Gamma)$ in Condition 2 of Definition 23, these are the sums that are subterms of terms in Γ. Condition 3 adds more "sums" in $sat(\Gamma)$, it tries to characterise a minimal number of sums that one needs to put in $sat(\Gamma)$, the bound we gave for our coefficients is loose. So, this definition of $sat(\Gamma)$ might not be the minimal one, but it contains a finite number of "sums" that is enough to generate all possible linear combinations that the intruder could build. If a bigger sum needs to be considered, it will be treated in Lemma 12. This condition of adding the linear combinations of terms in $sat(\Gamma)$ is fundamental to satisfy Condition 3 of Definition 12.

Proposition 18. *The set $sat(\Gamma)$ for E_{AG} given in Definition 23 is finite.*

Proof. To build $sat(\Gamma)$ one adds to the terms in Γ (which is finite), its public names, subterms, inverses and linear combinations of subterms, whose coefficients go up to the bound given by Proposition 17. □

Proposition 19. *The set $sat(\Gamma)$ for E_{AG} given in Definition 23 satisfies Condition 3 of Definition 12.*

ACCEPTED MANUSCRIPT

Proof. The proof can be found in the Appendix. □

Proposition 20. *The equational theory E_{AG} of Abelian Groups is* **N***-locally stable, and also* **I***-locally stable.*

Proof. It is enough to prove that the definition of $sat(\Gamma)$ for E_{AG} (Definition 23) satisfies all the conditions of Definition 12, since closure by inverses follows directly by definition and closure by linear combinations follows from Proposition 17.

First, the set for E_{AG} is finite by Proposition 18. Conditions 1, 2 and 5 are satisfied directly by the conditions in Definition 23. Condition 3 is satisfied by Proposition 19. Condition 4 is satisfied since, by Definition 23, we only include in the set terms that are in normal form. □

Theorem 21. *Let $\Gamma = \{M_1, \ldots, M_k\}$ be a finite set of ground terms in normal form and M a ground term in normal form. The* intruder deduction problem *for E_{AG} is decidable in polynomial time in $|M|$ and $|sat(\Gamma)|$.*

Proof. This theorem follows from Theorem 14, since E_{AG} is **I**-locally stable (Proposition 20). □

The analysis of this theory has been done in previous works, for more details check the Section 7 for related work and comparisons.

Remark 4. The set $sat(\Gamma)$ is exponential in size: by rule 3, one has to add all the linear combinations $(\alpha_1 N_1 \oplus \ldots \oplus \alpha_r N_r) \downarrow$ in $sat(\Gamma)$. Inspired by [14, 42], we can consider the DAG representation of $sat(\Gamma)$ with maximum sharing of terms, obtaining a polynomial (in $|\Gamma|$) representation of $sat(\Gamma)$. Therefore, the decidability could be computed in polynomial time with relation to the $|M|_{DAG}$ and $|sat(\Gamma)|_{DAG}$ by adapting the algorithm to work with DAGs (we will explore this approach in future work).

6.2. Abelian Groups plus Exponentiation

As in previous works, the theory E_{AG^h} (see Table 2) is used to analyse security properties of protocols that use exponentiation, for instance, El Gammal encryption and decryption schemes, RSA, Diffie-Hellman key agreement [21]. As in [13], we restrict the theory to exponentials with basis α (the generator of the multiplicative group of order p, namely, $\mathbb{Z}_p^*$, for some prime p), we consider the unary function symbol h defined as: $h(x) := \alpha^x$.

$x + (y + z) = (x + y) + z$	$i(i(x)) = x$	$j(h(x)) = h(i(x))$
$x + y = y + x$	$x \cdot 1 = x$	$h(0) = 1$
$x + 0 = x$	$j(x) \cdot x = 1$	$h(x + y) = h(x) \cdot h(y)$
$x + i(x) = 0$	$j(j(x)) = x$	$exp(h(x), y) = h(x \cdot y)$

Table 2: E_{AG^h}: Abelian Group and Exponentiation

The function symbol h has the homomorphism property: $h(x + y) = h(x) \cdot h(y)$, where $+$ is a binary symbol operator taken as *addition of exponents* and $\cdot$ is a binary symbol operator taken as *multiplication of exponentials*. The unary function symbols i and j are the inverses of $+$ and $\cdot$, respectively.

In the TRS $\mathcal{R}_{AG}^h$ defined below (see Table 3) only exponentials with base α will be considered, where α is the generator of the group $\mathbb{Z}_p^*$, for some prime number p.

ACCEPTED MANUSCRIPT

$x + 0 \to x$	$1 \cdot x \to x$	$h(x) \cdot h(y) \to h(x + y)$
$x + i(x) \to 0$	$j(x) \cdot x \to 1$	$exp(h(x), y) \to h(x \cdot y)$
$i(x + y) \to i(x) + i(y)$	$j(j(x)) \to x$	$j(h(x)) \to h(i(x))$
$i(i(x)) \to x$	$j(1) \to 1$	$exp(1, x) \to h(0 \cdot x)$
$i(0) \to 0$	$j(x \cdot y) \to j(x) \cdot j(y)$	$h(0) \to 1$

Table 3: $\mathcal{R}^h_{AG}$: Abelian Group and Exponentiation

Lemma 22. *$\mathcal{R}^h_{AG}$ is convergent modulo associativity and commutativity of $+$.*

Proof. Termination of $\mathcal{R}^h_{AG}$ is proved via the *recursive path order* with the order $j > i > exp > . > h > + > 1 > 0$ on the symbols of Σ^h_{AG}. Confluence was checked using CiME 3 [19]. □

Let $\oplus$ be an arbitrary AC function symbol in Σ_E for an equational theory E. Given a set S of terms and a set $\tilde{n}$ of private names, write $sum_\oplus(S, \tilde{n})$ for the set of arbitrary sums of terms in S and other names. We will define $sum_\oplus(S, \tilde{n})$ for $\oplus \in \{+, \cdot\}$ as follows

$$sum_+(S, \tilde{n}) = \left\{ \alpha_1 T_1 + \ldots + \alpha_k T_k + \beta_1 m_1 + \ldots + \beta_s m_s) \;\middle|\; \begin{array}{l} \alpha_i, \beta_j \in \mathbb{N} - \{0\} \\ k, s \in \mathbb{N} \\ m_i \in N - \tilde{n},\ T_i \in S \end{array} \right\}$$

$$sum_\bullet(S, \tilde{n}) = \left\{ T_1^{\alpha_1} \cdot \ldots \cdot T_r^{\alpha_r} \cdot m_1^{\beta_1} \cdot \ldots \cdot m_k^{\beta_k}) \;\middle|\; \begin{array}{l} \alpha_i, \beta_j \in \mathbb{N} - \{0\} \\ r, k \in \mathbb{N} \\ m_i \in N - \tilde{n},\ T_i \in S \end{array} \right\}$$

where αM counts for the term $M + \ldots + M$, α times ($\alpha \in \mathbb{N}$) and M^γ counts for $M \cdot \ldots \cdot M$, γ times ($\gamma \in \mathbb{N}$). Define $sum(S, \tilde{n}) = \bigcup_{i=1}^{k} sum_{\oplus_i}(S, \tilde{n})$, where $\oplus_1, \ldots, \oplus_k$ are the AC-symbols of the theory. Typically, the names in $\tilde{n}$ will be private and the others public.

By Definition 18 of ***I*-local stability** it is necessary to define an adequate "notion of subterms" based on the equational theory considered. We define a preliminary set of subterms which takes into account the *atoms* of "sums" and "multiplications" and the *arguments* of non-AC function symbols in the signature.

Definition 24. *Let t be a ground term in normal form. Define $S_{AG}(t)$ as*

1. *$t \in S_{AG}(t)$;*
2. *if $u = u_1 + u_2 + \ldots + u_n \in S_{AG}(t)$ then $atoms_+(u) \in S_{AG}(t)$.*
3. *if $u = u_1 \cdot u_2 \cdot \ldots \cdot u_n \in S_{AG}(t)$ then $atoms_\bullet(u) \in S_{AG}(t)$.*
4. *if $u = f(u_1, u_2) \in S_{AG}(t)$ then $u_1, u_2 \in S_{AG}(t)$, where $f \in \{exp, h, j\}$.*

This notion of subterms can be extended to a set T of ground terms in normal form in the usual way.

The second notion of subterms to be defined produces linear combinations of subterms from the previous set. This definition is used to generate partial sums that are subterms of bigger sums that appeared in an initial term or set of terms (for instance, Γ, the knowledge of the intruder).

ACCEPTED MANUSCRIPT

Definition 25 (SS_{AG^h})**.** *Let T be a finite set of ground terms in normal form. Define $SS_{AG^h}(T)$ as*

$$SS_{AG^h}(T) := \left\{ h\Big(\sum_{h(T_s)\cdot u_s \in M} \alpha_s \cdot T_s\Big) \cdot \prod u_s^{\gamma_s} \downarrow \;\middle|\; \begin{array}{c} M \subseteq S_{AG}(T), 1 \leq \alpha_s, \gamma_s \leq p-1 \\ h(T_s) \text{ or } u_s \text{ may be empty} \end{array} \right\}$$
$$\bigcup \left\{ \Big(\sum_{\substack{r \in M \\ r|_\varepsilon \neq h, exp, \cdot, j}} \beta_r \cdot r\Big) \downarrow \; | \, M \subseteq S_{AG}(T), 1 \leq \beta_r \leq p-1 \right\}$$

Definition 25 generates more combinations of subterms than necessary. In order to restrict it to subterms that may appear in a set T considered, the following definition will be adopted.

Definition 26 ($st_{E_{AG^h}}(T)$)**.** *Let T a set of ground terms in normal form, define $st_{E_{AG^h}}(T)$ as*

$$st_{E_{AG^h}}(T) := S_{AG}(T) \cup \left\{ M \in SS_{AG^h}(T) \,|\, M =_{AC} t_1|_p, \text{ for } t_1 \in S_{AG}(T) \text{ and } p \in \mathcal{P}os(t_1) \right\}$$

As in the theory of Abelian Groups, given a finite set Γ of ground terms in normal form, the set $sat(\Gamma)$ has to take into account the linear combinations

$$(\alpha_1 \oplus T_1 \oplus \ldots \oplus \alpha_r T_r) \downarrow \qquad (\oplus = \{+, \cdot\},\ T_1, \ldots, T_k \in sat(\Gamma)).$$

in order to obtain a saturation set satisfying the Condition 3 of the definition N-locally stable theories. The interesting case happens when $\oplus = \cdot$

In this case, the reduction in the head happens when, in the worst case scenario, $T_j = h(T'_j)$ for $j = 1, \ldots, k$. The linear combination can be rewritten as $(h(T'_1)^{\alpha_1} \cdot \ldots \cdot h(T'_k)^{\alpha_k}) \downarrow$. After consecutive applications of rule $h(x) \cdot h(y) \to h(x+y)$, it follows

$$h(T'_1)^{\alpha_1} \cdot \ldots \cdot h(T'_k)^{\alpha_k} \xrightarrow{*} h(\alpha_1 T'_1 + \ldots + \alpha_k T'_k) \xrightarrow{*} h((\alpha_1 T'_1 + \ldots + \alpha_k T'_k) \downarrow)$$

and the number of linear combinations w.r.t. + considered is finite, the technique to show this is the same as for the case of Abelian Groups. In addition, the group under consideration is finite, so one can restrict the coefficients to $1 \leq \alpha_i \leq p$, for $i = 1, \ldots, k$.

The set $st_{E^h_{AG}}$ of subterms will be used in the definition of the saturation set used to show that E^h_{AG} is **I**-locally stable.

Definition 27 ($sat(\Gamma)$ for E^h_{AG})**.** *Let $\Gamma = \{M_1, \ldots, M_n\}$ be a finite set of ground terms in normal form, define $sat(\Gamma)$ for E^h_{AG} as the smallest set generated by the following rules*

1. *$\Gamma \subseteq sat(\Gamma)$ and $e_\oplus \in sat(\Gamma)$ for each $\oplus \in \Sigma_E$ and $m \in sat(\Gamma)$ for every $m \in pn(\Gamma)$;*
2. *if $N_1, \ldots, N_k \in sat(\Gamma)$ and $f(N_1, \ldots, N_k) \in st_E(sat(\Gamma))$ then $f(N_1, \ldots, N_k) \in sat(\Gamma)$, for $f \in \Sigma_E$;*
3. *if $M \in sat(\Gamma)$ then $j(M)\downarrow, i(M)\downarrow \in sat(\Gamma)$.*
4. *if $M \in sat(\Gamma)$, and $M|_\varepsilon \neq h$ then $h(M)\downarrow \in sat(\Gamma)$.*
5. *if $N_1, N_2, \ldots, N_r \in sat(\Gamma)$ then $(\alpha_1 N_1 \oplus \ldots \oplus \alpha_r N_r)\downarrow \in sat(\Gamma)$, where $1 \leq \alpha_i \leq p$, $1 \leq i \leq r$ and $\oplus \in \{+, \cdot\}$.*

ACCEPTED MANUSCRIPT

6. *if* $N_1, N_2 \in sat(\Gamma)$ *such that* $N_2|_\varepsilon \neq h, exp$, $N_1 = h(N_1')$ *s.t.* $N_1'|_\varepsilon \neq +$ *and* $exp(N_1, N_2) \xrightarrow{h} M$ *via rule* $exp(h(x), y) \to h(x \cdot y)$ *then* $M \downarrow \in sat(\Gamma)$.

Remark 5. Conditions 1 and 2 are required for **N**-locally stable theories by Definition 12. Condition 3 is closing the terms by inverses of $\cdot$ and $+$. Condition 4 allows the computation of $h(N)$ whenever N is known by the intruder, the restriction to $N|_\varepsilon \neq h$ is to avoid double exponentiation, i.e., one does not apply exponentials of basis α to exponentials of basis α. Condition 5 takes into account the linear combinations necessary to satisfy the Condition 3 of Definition 12 mainly because of possible applications of rules: $h(x) \cdot h(y) \to h(x + y)$ and $x + i(x) \to 0$. Condition 6 also avoids double exponentiation.

The following two lemmas are technical and necessary to prove that the set $sat(\Gamma)$ defined for E_{AG^h} satisfies the conditions of Definition 12 (for **N**-locally stable theories).

Lemma 23. *The set* $sat(\Gamma)$ *for* E_{AG^h} *satisfies condition 3 of Definition 12.*

Proof. The proof is in the Appendix. □

Lemma 24. *The set* $sat(\Gamma)$ *for* E_{AG^h} *is finite.*

Proof. To build $sat(\Gamma)$ one adds elements of $st_{AG^h}(\Gamma)$ (by Condition 2 of Definition 27), their inverses (Condition 3), exponentials of basis α (Condition 4), and linear combinations and products of subterms. The only condition that could add an infinite number of terms in $sat(\Gamma)$ is Condition 5, however, since the group $\mathbb{Z}_p^*$ considered is finite, only a finite number of linear combinations will be added. □

Proposition 25. E_{AG^h} *is* ***I****-locally stable.*

Proof. It follows from Lemmas 23 and 24. □

Theorem 26. *Let* $\Gamma = \{M_1, \ldots, M_k\}$ *be a finite set of ground terms in normal form and* M *a ground term in normal form. The* Intruder Deduction Problem *for* E_{AG^h} *is decidable in polynomial time in* $|M|$ *and* $|sat(\Gamma)|$.

This equational theory has been analysed in previous works, a comparison with other works can be found in Section 7.

In order to obtain polynomial bounds, one can follow the suggestion in Remark 4.

6.3. XOR

Using the same methods, one can show that the theory of XOR, E_{XOR}, is **I**-locally stable. The equational theory E_{XOR} is axiomatised by the following equations.

$$E_{XOR} = \left\{ \begin{array}{rcl@{\qquad}rcl} x \oplus y & = & y \oplus x & x \oplus 0 & = & x \\ x \oplus (y \oplus z) & = & (x \oplus y) \oplus z & x \oplus x & = & 0 \end{array} \right\}$$

We can also add an inverse symbol i, with the equation $i(x) = x$ to satisfy the requirements of **I**-locally stable theories.

The term rewriting system $\mathcal{R}_{XOR}$ associated to E_{XOR} is given in Figure 1.

The notion of subterms st_{XOR} can be defined similarly to the notion previously defined for the theory E_{AG}.

ACCEPTED MANUSCRIPT

$x \oplus 0 \to x$	$x \oplus x \to 0$	$i(x) \to x$

Figure 1: $\mathcal{R}_{XOR}$- a term rewriting system for E_{XOR}

Definition 28 ($S_{XOR}(T)$)**.** *Let t be a ground term in normal form, define $S_{XOR}(t)$ as*

- $t \in S_{XOR}(t)$
- *if $u = u_1 \oplus u_2 \oplus \ldots \oplus u_n \in S_{XOR}(t)$ then $atoms(u) \subset S_{XOR}(t)$.*

This notion can be extended for a set T of ground terms in normal form in the usual way: $S_{XOR}(T) := \bigcup_{t \in T} S_{XOR}(t)$

Notice that, the size of $S_{XOR}(T)$ is linear in the size of T (here the size of a term stands for the number of symbols appearing in it).

The set SS_{XOR} contains the linear combinations of the terms in $S_{XOR}(T)$.

Definition 29 ($SS_{XOR}(T)$)**.** *Let T be a finite set of ground terms in normal form, define $SS_{XOR}(T)$ as*

$$SS_{XOR}(T) := \left\{ \bigoplus_{s \in M} s \mid M \subseteq S_{XOR}(T) \right\}$$

The size of $SS_{XOR}(T)$ is exponential in the size of $S_{XOR}(T)$, it is enough to consider the fact that there are $2^{|S_{XOR}(T)|}$ possible subterms M.

Definition 30 (st_{XOR})**.** *Let T be a set of ground terms in normal form, define $st_{XOR}(T)$ as*

$st_{XOR}(T) := \{M \in SS_{XOR}(T) \mid M =_{AC} t|_p$, for a term $t \in S_{XOR}(T)$ and some $p \in \mathcal{P}os(t)\} \cup S_{XOR}(T)$

Definition 31 ($sat(\Gamma)$ for XOR)**.** *Given a set $\Gamma = \{M_1, \ldots, M_k\}$ of ground terms in normal form, $sat(\Gamma)$ is the smallest set generated by the following rules*

1. $\Gamma \subseteq sat(\Gamma)$ *and* $m \in sat(\Gamma)$ *for every* $m \in pn(\Gamma)$*;*
2. $N_1, \ldots, N_t \in sat(\Gamma)$ *and* $f(N_1, \ldots, N_t) \in st_{XOR}(\Gamma)$ *then* $f(N_1, \ldots, N_t) \in sat(\Gamma)$*,* $f \in \Sigma_{XOR}$*.*
3. *if* $N_1, N_2 \in sat(\Gamma)$ *and* $N_1 \oplus N_2 \xrightarrow{h} M$ *via rule* $x \oplus x \to 0$ *then* $M{\downarrow} \in sat(\Gamma)$*.*

Proposition 27. *The set $sat(\Gamma)$ defined for the theory E_{XOR} satisfies Condition 3 of the Definition 12.*

Proof. This proof is similar to the case of Abelian Groups and can be found in [36]. □

Lemma 28. *The theory E_{XOR} is **I**-locally stable.*

Proof. Since every term in $sat(\Gamma)$ is its own inverse, it is sufficient to show that the set $sat(\Gamma)$ specified in Definition 31 for the theory E_{XOR} satisfies the conditions (1-5) of the definition of **N**-locally stable theories (Definition 12). Conditions 1, 2, 4 and 5 are satisfied by Definition 31. Note that whenever $M \in sat(\Gamma)$ it follows that $M{\downarrow} \in sat(\Gamma)$: Γ contains only normal forms therefore condition 2 adds only normal forms and condition 3 adds the normal forms of linear combinations $\alpha_1 N_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_r N_r$ of terms in $sat(\Gamma)$, with $\alpha_i = 0, 1$. □

ACCEPTED MANUSCRIPT

For the procedure for AC matching (Lemma 12), we remark for the theory E_{XOR} we obtain a system of linear Diophantine equations over $\mathbb{Z}/2\mathbb{Z}$ which can be solved in polynomial time using Gaussian elimination. A similar approach is used in [31].

Theorem 29 (Decidability of IDP for XOR)**.** *Let* $\Gamma = \{M_1, \ldots, M_k\}$ *be a finite set of ground terms in normal form and* M *a ground term in normal form. The* intruder deduction problem *for* E_{XOR} *is decidable in polynomial time in* $|M|$ *and* $|sat(\Gamma)|$.

Proof. The result is a consequence of Lemma 28 and Theorem 14, where the domain of the SLDE obtained for this theory is $\mathbb{Z}/2\mathbb{Z}$. □

This equational theory has been analysed in previous works, a comparison with other works can be found in Section 7.

In order to obtain polynomial bounds, one can follow the suggestion in Remark 4.

7. Related Work

The analysis of cryptographic protocols has attracted a lot of attention in the last years and several tools are available to try to identify possible attacks, see Maude-NPA [25], ProVerif [11], Avispa [3], Yapa [8].

Abadi and Cortier in [1] propose a methodology to decide the message deducibility relation for the class of locally stable theories. More precisely, they state that given a frame ϕ and a term M, once $M\downarrow$ and $sat(\phi)$ are computed, $\phi \vdash M$ can be decided in polynomial time in $|M\downarrow|$ and $|sat(\phi)|$ (Theorem 2, page 23 [1]), where $M\downarrow$ represents the set of normal forms of M modulo associativity and commutativity of some AC-operator. The idea is that $\phi \vdash M$ can be decided by checking whether one of the terms in $M\downarrow$ is of the form $C[M_1, \ldots, M_k]$ with $M_i \in sat(\phi)$ (Proposition 16 [1], page 24). Regarding the complexity of the algorithm, once $M\downarrow$ and $sat(\phi)$ are computed, [1] states that $\phi \vdash M$ can be decided in polynomial time in $|M\downarrow|$ and $|sat(\phi)|$ using the same procedure as for Theorem 1 (page11 [1]), proposed initially for convergent subterm theories.

To highlight the differences between the algorithm proposed in [1] and the one given in this paper, we use an example.

Example 10. Let E_{AC} be the *pure AC* theory. It was stated in Section 5.2.5 of [1] that this theory is locally stable and in Subsection 4.3 of this paper that it is **N**-locally stable. Consider the following set:

$$\Gamma = \left\{ \begin{array}{l} n_1 \oplus n_{10} \oplus n_9 \oplus n_7 \oplus n_8 \ ,\ n_2 \oplus n_6 \oplus n_4 \oplus n_9 \oplus n_7 \ ,\ n_2 \oplus n_3 \oplus n_5 \oplus n_7 \oplus n_8, \\ n_2 \oplus n_3 \oplus n_5 \oplus n_6 \oplus n_9 \ ,\ n_4 \oplus n_3 \oplus n_9 \oplus n_6 \oplus n_1, \\ n_1 \oplus n_4 \oplus n_2 \oplus n_9 \ ,\ n_1 \oplus n_3 \oplus n_5 \oplus n_6 \ ,\ n_1 \oplus n_4 \oplus n_2 \oplus n_9 \ ,\ n_2 \oplus n_7 \oplus n_4 \oplus n_3 \ , \\ n_3 \oplus n_{10} \oplus n_8 \oplus n_7, \\ n_5 \oplus n_7 \oplus n_3 \ ,\ n_7 \oplus n_6 \oplus n_5 \ ,\ n_1 \oplus n_2 \oplus n_3, \\ n_1 \oplus n_4 \ ,\ n_7 \oplus n_4 \ ,\ n_2 \oplus n_5 \ ,\ n_7 \end{array} \right\}$$

The set $sat(\Gamma) = \Gamma \cup \{n_2 \oplus n_5 \oplus n_7\} \cup [\Gamma \cup \{n_2 \oplus n_5 \oplus n_7\}]_{\approx_{AC}}$, satisfies the definition of $sat(\Gamma)$ in [1]. Here, $[\Gamma]_{\approx_{AC}}$ stands for the equivalence class of Γ modulo AC.

Let $M = n_1 \oplus n_7 \oplus n_5 \oplus n_4 \oplus n_6 \oplus n_3 \oplus n_2 \oplus n_9$ be a ground term in normal form.

Following the approach in [1] one wants to find terms $T_1, \ldots, T_k \in sat(\Gamma)$ and a context C such that $M == C[T_1, \ldots, T_k]$.

ACCEPTED MANUSCRIPT

1. Starting with $T_1 = n_1 \oplus n_{10} \oplus n_9 \oplus n_7 \oplus n_8$ one can verify that there is no subterm in M which is equal (syntactically) to T_1. The answer is NO.

2. Go to the next term $T_2 = n_2 \oplus n_6 \oplus n_4 \oplus n_9 \oplus n_7$.

   Notice that the term $M_1 = \mathbf{n_2} \oplus \mathbf{n_6} \oplus \mathbf{n_4} \oplus \mathbf{n_9} \oplus \mathbf{n_7} \oplus n_1 \oplus n_5 \oplus n_3 \in M\downarrow$. Following the procedure, we now delete T_2 from M_1obtaining $M_1 = \Box \oplus n_1 \oplus n_5 \oplus n_3$ and run the procedure again for $M_1' = n_1 \oplus n_5 \oplus n_3$. There is no term in $sat(\Gamma)$ that matches (syntactically) the remaining part of M_1'. The answer is NO.

3. Go to the next term $T_3 = n_2 \oplus n_3 \oplus n_5 \oplus n_7 \oplus n_8$, one can verify that there is no subterm in M which is equal to T_3. The answer is NO.

4. Go to the next term $T_4 = n_2 \oplus n_3 \oplus n_5 \oplus n_6 \oplus n_9$.

   Notice that the term $M_2 = \mathbf{n_2} \oplus \mathbf{n_3} \oplus \mathbf{n_5} \oplus \mathbf{n_6} \oplus \mathbf{n_9} \oplus n_1 \oplus n_7 \oplus n_4 \in M\downarrow$. Following the procedure, we now delete T_4 from M_2 obtaining the term $M_2 = \Box \oplus n_1 \oplus n_7 \oplus n_4$ and run the procedure again for $M_2' = n_1 \oplus n_7 \oplus n_4$. Following this reasoning we conclude the term to be matched first is $T_5 == n_1 \oplus n_4$ followed by $T_6 == n_7$ we get a positive answer.

The algorithm suggested in [1] tries the terms in the congruence class modulo AC of M until there is one that matches syntactically with the terms in $sat(\Gamma)$. In the worst case scenario, a exponential number of terms will be considered. Given one term in $M\downarrow$, the analysis is done in polynomial time. Therefore the whole procedure is polynomial in $|M\downarrow|$ (here $|M\downarrow|$ represents the cardinality of the set $M\downarrow$) and $|sat(\Gamma)|$.

Theorem 1 [1] says: *"This procedure is correct because, when cutting subterms of M equal to terms in sat*(Γ)*, we start with terms in sat*(Γ) *of maximal size"*.

Consider now the definition of $sat(\Gamma)$ for E_{AC} given in this paper (Definition 17). In this example $sat(\Gamma) = \Gamma \cup \{n_2 \oplus n_5 \oplus n_7\}$ since $n_2 \oplus n_5, n_7 \in sat(\Gamma)$ and $(n_2 \oplus n_5) \oplus n_7 \in st_{AC}(sat(\Gamma))$.

Using the algorithm proposed in Lemma 15, to check decidability of $M =_{AC} C[T_1, \ldots, T_k]$ for $T_1, \ldots, T_k \in sat(\Gamma)$ one has to solve the Diophantine equation corresponding to: $\beta_1 T_1 + \beta_2 T_2 + \ldots + \beta_k T_k = M$, for $\beta_1, \ldots, \beta_k \in \mathbb{N}$. Following the procedure proposed in the proof of Lemma 12, one can transform the equation above in a system of equations with natural coefficients. The solvability can be decided in non-deterministic polynomial time in $|M|$ and $|sat(\Gamma)|$.

For **N-**locally stable theories it seems that there is no much gain in using the AC-matching algorithm proposed in Lemma 15 for $\mathbb{N}$. The difference is for **I**-locally stable theories:

- the procedure proposed in [1] still has to perform the syntactic check for all elements in the congruence class modulo AC of a term M, providing a polynomial in $|M\downarrow|$ and $|sat(\Gamma)|$ (where both sets have exponential size) decidability of deduction.

- The algorithm in Lemma 12 can decide the same problem in polynomial time in $|M|$ and $|sat(\Gamma)|$.

So far, many theoretical results related to the decidability of IDP under equational theories have been obtained. The theory of Abelian Groups has attracted a lot of attention since, combined with other properties, it is part of the structure of many cryptographic algorithms (eg. SALARY SUM, IKA.1, MAKEP [21]).

ACCEPTED MANUSCRIPT

7.1. AG: Comparison with [18, 15, 32, 23, 35]

The IDP for Abelian Groups (and XOR) can be decided in non-deterministic polynomial time; Comon-Lundh and Shmatikov [18] prove this result using the strategy of normal proofs and McAllester's locality property [34].

The decidability of IDP for AC-theories with homomorphism is studied in [32]. The approach proposed is based on McAllester's locality property working basically with proof transformations pioneered by Gentzen. It is also stated that IDP for the theory of Abelian Groups is decidable in polynomial time using the same approach, but this fact has not been shown in the paper. We noticed that the proposed technique extends the notion of syntactic subterms to a wider one, which is consistent with the axioms of associativity and commutativity, obtaining a set of subterms whose size is exponential w.r.t. the size of the initial knowledge of the intruder. Therefore, *within this approach* the decidability of IDP would be exponential w.r.t the size of the subterms.

In [23], the authors prove the decidability of IDP for AGh (Abelian Groups with homomorphism). The method is based on the Dolev-Yao model of the intruder, together with McAllester's locality property [34], where the one step-deducibility is checked using an algorithm for deciding equality modulo E. Our method reduces the problem of deciding equality modulo E to the problem of deciding matching modulo AG, which can be decided in polynomial time for a restricted case of AG-unification problem [7]. One can prove that AGh is an **I**-locally stable theory following the steps shown in this paper. To bound the size of $sat(\Gamma)$ for this theory, one can follow the method suggested by [14], considering its DAG representation.

Millen and Shmatikov [35] investigate a constraint solving technique that reduces the *security problem for active intruders* for Abelian Groups to a system of quadratic Diophantine equations, but the decidability was obtained by Shmatikov in [38], by reducing the initial problem to the solvability of a particular system of quadratic Diophantine equations, for the case of bounded number of sessions.

7.2. AG + exponentiation: Comparison with [13, 30]

The IDP for the equational theory modelling an electronic purse protocol was investigated in [13]. This theory consists of rules for Abelian Groups and Exponentiation. The authors show that the TRS associated satisfies the Finite Variant Property, and they prove that the equational theory is *local* in the sense of McAllester [34]. However, they need to define, for each message M for which one is interested in checking the IDP a saturation set, called *notion of subterms*. In this work we build only one saturation set, for a given Γ, that can be used for each message that one wants to check the IDP problem. Our saturation set depends on the rewrite rules associated to the equational theory, while their notion of subterms is more connected to the structure of subterms. The notion of subterms defined in [13] was not enough for the purpose of the work, and an alternative notion was given in [37].

Differently from [30], the equational theory for Abelian Groups with exponentiation considered here is a bit more restricted. We only consider exponentials with a fixed basis, with this we obtain the decidability of unification, as it was suggested in [13].

Sequent calculus formulations of Dolev Yao intruders [41] have been used in a formulation of open bisimulation for the spi-calculus. In [42], deductive techniques for dealing with a protocol with blind signatures in mutually disjoint AC-convergent equational theories, containing a unique AC operator each, are considered. As an alternative approach, the intruder's deduction capability is modelled inside a sequent calculus modulo a rewriting system, following the approach of [9]. Then, the IDP is reduced in polynomial time to EDP.

ACCEPTED MANUSCRIPT

By combining the techniques in [42] and [13], the IDP formulation for an Electronic Purse Protocol with blind signatures was proved to reduce in polynomial time to EDP for an AC-convergent theory containing three different *AC* operators and rules for exponentiation [37], extending the previous results. However, no algorithm was provided to decide EDP. More precisely, assuming that EDP is solved in time $O(f(n))$, it was proved that IDP reduces polynomially to EDP with complexity $O(n^k \times f(n))$, for some constant k. Thus, whenever the former problem is polynomial, the IDP is also polynomial.

7.3. XOR: Comparison with [14, 23]

In [14], the authors propose methods for proving that the *protocol insecurity problem* is in NP for an intruder that can exploit properties of the XOR operator. As a consequence of this result, the IDP for an intruder using XOR is in PTIME. This approach uses oracle rules and also one-step deducibility. Using a different approach, the decidability of IDP for XOR with homomorphism (ACUNh) is shown to be in PTIME in [23].

Using our framework it is possible to prove that the IDP for XOR is decidable in polynomial time w.r.t a saturated set of subterms, since this theory is a member of the class of the **I**-locally stable theories. It is possible to show that ACUNh is **I**-locally stable, and therefore is decidable in polynomial time in $|M|$ and $|sat(\Gamma)|$. In addition, following the approach in [14], and considering the DAG representation of $|M|$ and $|sat(\Gamma)|$, one can prove the decidability of IDP in PTIME.

8. Conclusion

This paper presents a method to decide the *intruder deduction problem* for equational theories that include associative and commutative axioms, namely the **N**-locally stable theories. Our method is based on a refined notion of the "locally stable theories", namely the **N**- and **I**-locally stable theories. The notion of "local stability" was first introduced by M. Abadi and V. Cortier in [1] in the context of the applied pi calculus.

We have defined the class of **I**-locally stable theories, which is a subclass of **N**-locally stable theories which contain inverses. We have proposed an algorithm to solve a restricted case of higher-order AG-matching by using a technique to decide a restricted case of AG-unification problem [7] combined with an algorithm to solve linear Diophantine equations over $\mathbb{Z}$. This algorithm runs in polynomial time w.r.t a saturated set for the class of **I**-locally stable theories. The algorithm can be adapted for **N**-locally stable theories without inverses, it relies on solving linear Diophantine equations over $\mathbb{N}$ which is an NP -complete problem. Our algorithm does not need to compute the set of normal forms modulo AC of a given term (which may be exponential).

We apply the results to the equational theory of Abelian Groups, Abelian Groups with Exponentiation, XOR and Pure AC. The first and second theories are **I**-locally stable, therefore the IDP is decidable in polynomial time w.r.t a saturated set of subterms. The third theory can be proven to be **I**-locally stable following the same technique. Finally, the fourth theory is **N**-locally stable, therefore, the IDP, in this case, is decidable in nondeterministic polynomial time w.r.t a saturated set of subterms.

9. Acknowledgements

We would like to thank Delia Kesner and the anonymous referees for important comments and remarks.

ACCEPTED MANUSCRIPT

References

[1] M. Abadi and V. Cortier. *Deciding knowledge in security protocols under equational theories.* In *Theoretical Computer Science*, 367(1-2):2–32, 2006.

[2] M. Abadi and C. Fournet. *Mobile Values, New Names, and Secure Communication.* In *Proc. 28th Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115,ACM, 2001.

[3] A. Armando *et al*. *The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications.* In *Proc. 17th Computer Aided Verification (CAV'05)*, vol. 3576 of *LNCS*, pages 281–285. Springer-Verlag 2005.

[4] M. Arnaud, V. Cortier and S. Delaune. *Deciding Security for Protocols with Recursive Tests.* In *Proc. of 23rd Int. Conference on Automated Deduction (CADE)*, vol. 6803 of *LNCS*, pages 49–63, Springer, 2011.

[5] M. Ayala-Rincón, M. Fernández and D. Nantes-Sobrinho. *Elementary Deduction for Locally Stable Theories with Normal Forms.* In *Proc. of 7th Workshop on Logical and Semantic Frameworks, with Applications (LSFA'12)*, vol 113 of *EPTCS*, pages 45–60, 2012.

[6] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[7] F. Baader and W. Snyder. *Unification Theory.* In *Handbook of Automated Reasoning*, vol. 1, Chapter 8, pages 445-532, Elsevier and MIT Press, 2001.

[8] M. Baudet, V. Cortier and S. Delaune. *YAPA: A Generic Tool for Computing Intruder Knowledge.* In *ACM Transactions on Computational Logic*, vol. 14(1), pages 4:1–4:32, 2013.

[9] V. Bernat and H. Comon-Lundh. *Normal proofs in intruder theories.* In *Advances in Computer Science - ASIAN 2006. Secure Software and Related Issues*, vol. 4435 of *LNCS*, pages 151–166. Springer, 2006.

[10] M. Berrima, N. B. Rajeb and V. Cortier. *Deciding knowledge in security protocols under some e-voting theories.* In *RAIRO - Theoretical Informatics and Applications*, vol. 45(3), pages 269–299, 2011.

[11] B. Blanchet. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules.* In *Proc. 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, pages 82–96, IEEE Comp. Soc. , 2001.

[12] A. Boudet, E. Contejean and H. Devie. *A new AC Unification Algorithm with an Algorithm for Solving Systems of Linear Diophantine Equations.* In *Proc. 5th Annual Symposium on Logic in Computer Science (LICS'90)*, pages 289–299, IEEE Comp. Soc., 1990.

[13] B. Bursuc, H. Comon-Lundh, and S. Delaune. *Deducibility constraints, equational theory and electronic money.* In *Rewriting, Computation and Proof*, vol. 4600 of *LNCS*, pages 196–212. Springer, 2007.

[14] Y. Chevalier, R. Kusters, M. Rusinowitch and M. Turuani. *An NP decision procedure for protocol insecurity with XOR.* In *Theoretical Computer Science*, vol. 338(1–3), pages 247—274, 2005.

[15] Y. Chevalier, R. Kusters, M. Rusinowitch and M. Turuani. *Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents.* In *Proc. of 23rd Foundations of Software Technology and Theoretical Computer Science (FSTTCS'03)*, vol. 2914 of *LNCS*, pages 124–135, Springer, 2003.

[16] D. Chaum *Blind Signatures for Untraceable Payments.* In *Proceedings of Advances in Cryptology (CRYPTO'82)*, pages 199–203, Plenum Press, New York, 1982.

[17] M. Clausen and A. Fortenbacher. *Efficient Solution of Linear Diophantine Equations.* In *Journal of Symbolic Computation*, vol. 8(1-2), pages 201–216, 1989.

[18] H. Comon-Lundh and V. Shmatikov. *Intruder Deduction, Constraint Solving and Insecurity Decisions in Presence of Exclusive or.* In *Proc. of 18th Annual Symposium on Logic in Computer Science (LICS'03)*, pages 271–280, IEEE Comp. Soc., 2003.

[19] E. Contejean, P. Courtieu, J. Forest, O. Pons and X. Urbain *The CiME rewrite tool (version 3)*, 2011.

[20] V. Cortier and S. Delaune. *Decidability and Combination Results for Two Notions of Knowledge in Security Protocols.* In *Journal of Automated Reasoning*, vol. 48(4), pages 441–487, 2012.

[21] V. Cortier, S. Delaune, and P. Lafourcade. *A survey of algebraic properties used in cryptographic protocols.* In *Journal of Computer Security*, vol. 14(1), 1–43, 2006.

[22] S. Delaune. *Vérification des protocoles cryptographiques et propriétés algébriques*. PhD thesis, École Normale Supérieure de Cachan, 2006.

[23] S. Delaune. *Easy Intruder Deduction Problems with Homomorphisms. Information Processing Letters*, vol. 97(6), pages 213–218, 2006.

[24] D. Dolev and A. Yao. *On the security of public keys protocols.* In *IEEE Trans. Information Theory*, vol. 29(2), pages 198–207, 1983.

[25] S. Escobar, C. Meadows and J. Meseguer. *Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties.* In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, vol. 5705 of *LNCS*, pages 1–50, Springer, 2009.

[26] M. A. Frumkin. *Polynomial time Algorithms in the Theory of Linear Diophantine Equations.* In *Proc. of Fundamentals of Computation Theory (FCT)*, vol. 56 of *LNCS*, 386–392, Springer, 1977.

[27] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-completeness.* W. H. Freeman and Co., 1979.

ACCEPTED MANUSCRIPT

[28] J. Giesl, R. Thiemann, P. Schneider-Kamp, and S. Falke *Automated Termination Proofs with AProVE.* In *Proc. of the 15th Int. Conference on Rewriting Techniques and Applications (RTA'04)*, vol. 3091 of *LNCS*, 210–220, 2004.
[29] G. Huet. *An Algorithm to Generate the Basis of Solutions to Homogeneous Linear Diophantine equations. Information Processing Letters*, vol. 7(3), pages 144–147, 1978.
[30] D. Kapur, P. Narendran, and L. Wang. *An E-unification algorithm for analyzing protocols that use modular exponentiation.* In *Proc. of International Conference on Rewriting Technique and Applications (RTA'03)*, vol. 2706 of *LNCS*, pages 165–179, Springer, 2003.
[31] Pascal Lafourcade. *Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption.* In *Electronic Notes in Theoretical Computer Science*, vol. 171(4), pages 37–57, 2007.
[32] P. Lafourcade, D. Lugiez and R. Treinen. *Intruder Deduction for AC-Like Equational Theories with Homomorphisms.* In *Proc. of 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, vol. 3467 of *LNCS*, pages 308–322, Springer, 2005.
[33] P. Lafourcade. *Intruder Deduction for the equational theory of exclusive-or with commutative and distributive encryption.* In *Electronic Notes on Theoretical Computer Science*, vol. 171(4), pages 37–57, 2007.
[34] D. McAllester. *Automatic recognition of tractability in inference relations.* In *Journal of the ACM*, vol. 40, pages 284–303, 1990.
[35] J. K. Millen and V. Shmatikov. *Symbolic protocol analysis with an Abelian group operator or Diffie-Hellman exponentiation.* In *Journal of Computer Security*, vol. 13 (3), pages 515–564, 2005.
[36] D. Nantes-Sobrinho. *O Problema da Dedução do Intruso para Teorias AC-convergentes Localmente Estáveis.* PhD Thesis, Departmento de Matemática, Universidade de Brasília, 2013. In Portuguese.
[37] D. Nantes-Sobrinho and M. Ayala-Rincón. *Reduction of the Intruder Deduction Problem into Equational Elementary Deduction for Electronic Purse Protocols with Blind Signatures.* In *Proc. of 17th Workshop on Logic, Language, Information and Computation (WoLLIC'10)*, vol. 6188 of *LNCS*, pages 218–231, Springer, 2010.
[38] V. Shmatikov. *Decidable Analysis of Cryptographic Protocols with Products and Modular Exponentiation.* In *13th European Symposium on Programming (ESOP'04)*, vol. 2986 of *LNCS*, pages 355–369, Springer, 2004.
[39] A. Schrijver. *Theory of Linear and Integer Programming. Wiley-Interscience in Discrete Mathematics and Optimization*, 1998.
[40] C. Papadimitriou. *Computational Complexity.* Addison-Wesley, Inc, 1994.
[41] A. Tiu. *A trace based simulation for the spi calculus: An extended abstract.* In *Proc. 5th Asian Symposium of Programming Languages and Systems (APLAS'07)*, vol. 4807 of *LNCS*, pages 367–382, Springer, 2007.
[42] A. Tiu, R. Goré and J. E. Dawson. *A proof theoretic analysis of intruder theories.* In *Logical Methods in Computer Science*, vol. 6(3), 2010.
[43] H. Zankl, B. Felgenhauer, A. Middeldorp. CSI- A confluence tool. In *Proc. 23rd International Conference on Automated Deduction (CADE'11)*,vol. 6803 of *LNCS (LNAI)*,499–505, 2011.

Appendix A. Proof of Lifting Lemma (Lemma 3)

The following lemma suggests a strategy to minimise the contexts in terms of the form $C[T_1, \ldots, T_k]$, where $T_1, \ldots, T_k \in sat(\Gamma)$, by checking which subterms $C|_p[T_1, \ldots, T_k]$ for some p are in $sat(\Gamma)$ and taking this subcontext as $\Box$. This result was stated in [1] in the proof of Lemma 11 [1], here we present an alternative proof.

Lemma 30 (Minimising contexts)**.** *Let E be a $\mathbf{N}$-locally stable theory, C an AC-normal context and $T_1, \ldots, T_k \in sat(\Gamma)$. If there is a position p in C such that $C|_p \neq \Box$ and there exists a non-empty position q such that $C|_{pq} = \Box$ and $C[T_1, \ldots, T_k]|_p \in sat(\Gamma)$, then $C' \stackrel{def}{=} C[p \leftarrow \Box]$ is an AC-normal context and $|C'| < |C|$.*

Proof. The proof follows by searching for a maximal position $p \in \mathcal{P}os(C)$ in the tree representation of C such that $C[T_1, \ldots, T_k]|_p \stackrel{def}{=} A$ and $A \in sat(\Gamma)$. One considers a new context C' which will be constructed by replacing $C|_p$ for a hole which will be instantiated with A. That is, $C[T_1, \ldots, T_k] == C'[T_{i_1}, \ldots, \underbrace{A}_{\text{position}-p}, \ldots, T_{i_r}]$ where $T_{i_1}, \ldots, T_{i_r} \in \{T_1, \ldots, T_k\}$ and C' is a context strictly smaller than C.

ACCEPTED MANUSCRIPT

Suppose that the context $C' = C[p \leftarrow \Box]$ is not in normal form. Since, the only change made in the context C happened in the branch ending in the position p, it follows that, there is a rewriting reduction in this branch after replacing $C|_p$ with $\Box$. Therefore, there is a position q in C such that $p = qj$, for some j, and $C|_q$ is reducible, contradicting the assumption. Therefore, C' is an AC-normal context. □

Remark 6. Notice that if there exist another position $p' \in \mathcal{P}os(C')$ satisfying the hypothesis of the Lemma 30 it is possible to execute the transformation again. Since p is maximal, one has that p' is parallel to p. Iterating the process (or executing transformations in parallel) one obtains a minimal context for C and $T_1, \ldots, T_k$.

The following lemma characterizes the structure of a context whose holes were instantiated with terms from $sat(\Gamma)$ and that contains a reducible subterm (using the rewrite system associated to the equational theory E), assuming the theory E is **N**-locally stable. The statement of this lemma was presented in the proof of Lemma 11 [1]. The proof relies on analysing the structure of the rewrite rule $M_0 \rightarrow N_0 \in \mathcal{R}_E$ applied on $C[T_1, \ldots, T_k] \rightarrow T$ (hypothesis of the lemma) as well as on the signature of the equational theory E.

We assume that the contexts used in the Lemma 31 do not contain private names, that is, $pn(C) \cap \tilde{n} = \emptyset$ for all context C used.

Lemma 31 (Structural Characterisation of Redexes)**.** *Let E be an* **N***-locally stable theory. Let C be an AC-normal context and $T_1, \ldots, T_k \in sat(\Gamma)$ such that $C[T_1, \ldots, T_k] \rightarrow T$ via rule $M_0 \rightarrow N_0 \in \mathcal{R}_E$. Then, the term $C[T_1, \ldots, T_k]$ can be written as*

$$C[T_1, \ldots, T_k] =_{AC} C^*[T_{j_1}, \ldots, T_{j_s}, \underbrace{M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]}_{\text{position } q}, T_{j_{s+1}} \ldots, T_{j_w}] \qquad \text{(A.1)}$$

where C'_i and C^* are contexts and q is a position in $C[T_1, \ldots, T_k]$. The terms $M' = M'_1 \oplus \ldots \oplus M'_t$, and $M'' = M''_1 \oplus \ldots \oplus M''_l$ for $t \leq l$ are [10] *such that $M'_u \oplus M''_u \in sat(\Gamma)$ and $M''_{t+1}, \ldots, M''_l \in sat(\Gamma)$* [11]*. For each i, $C'_i|_\varepsilon \neq \oplus$ and $T_{j_1}, \ldots, T_{j_w}, T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$.*

In addition, $M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}] =_{AC} M_0\theta$ for $r' \leq r$ and some substitution θ.

Proof. The proof follows by analysing the structure of the rule $M_0 \rightarrow N_0$ from $\mathcal{R}_E$ that is applicable in $C[T_1, \ldots, T_k]$ and the corresponding structure that this term has to have in order to have a reducible subterm. Consider the representation of the (lhs) of the rule $M_0 \rightarrow N_0$ via a context whose holes were instantiated with the variables from $\mathcal{V}ar(M_0)$: $M_0 = C_{M_0}[x_1, \ldots, x_{k_0}]$ where C_{M_0} is an context and $x_1, \ldots, x_{k_0} \in \mathcal{V}ar(M_0)$, suppose that the variable positions are respected as well as their repetitions. Since the rule $M_0 \rightarrow N_0$ is applicable in $C[T_1, \ldots, T_k]$ there exists a position p such that $C[T_1, \ldots, T_k]|_p =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$. for some substitution θ.

Case 1. Suppose that $C_{M_0}|_\varepsilon = f$, for some $f \in \Sigma_E$ such that $f \neq \oplus$.

Suppose that f is a n-ary function symbol, for some $n \in \mathbb{N}$. Then, $C[T_1, \ldots, T_k]|_p = f(C_1[T_{1_1}, \ldots, T_{1_{r_1}}], \ldots, C_n[T_{n_1}, \ldots, T_{n_{r_n}}])$ where $C_1, \ldots, C_n$ are contexts with $pn(C_i) \cap \tilde{n} =$

[10] The case where $l \leq t$ is analogous.

[11] $1 \leq i \leq r$, $r \in \mathbb{N}$, $t \in \mathbb{N}$, $l \in \mathbb{N}$, $1 \leq u \leq t$.

ACCEPTED MANUSCRIPT

$\emptyset$, $p \in \mathcal{P}os(C)$ and $T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}} \in \{T_1, \ldots, T_k\}$. To facilitate the notation, write: $f(C_1[T_{1_1}, \ldots, T_{1_{r_1}}], \ldots, C_n[T_{n_1}, \ldots, T_{n_{r_n}}]) = C_p[T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}}]$. Hence, $C[T_1, \ldots, T_k] =_{AC} C^*[\ldots, \underbrace{C_p[T_{1_1}, \ldots, T_{1_{r_1}}, \ldots, T_{n_1}, \ldots, T_{n_{r_n}}]}_{\text{position } p}, \ldots]$.

And the result follows for $r = 1$ and terms M' and M'' empty in (A.1).

Case 2. Suppose that $C_{M_0}|_\varepsilon = \oplus$.

By induction on the number of occurrences of $\oplus$ in C_{M_0} one can prove that $C[T_1, \ldots, T_k]|_p$ has the following form: $C[T_1, \ldots, T_k]|_p = R \oplus \bigoplus_{i=1}^{s} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]$,

for contexts C'_i with $pn(C'_i) \cap \tilde{n} = \emptyset$ $(1 \leq i \leq r)$ such that $C'_i|_\varepsilon \neq \oplus$ and some $s \in \mathbb{N}$. In addition, a term $R = M'_1 \oplus \ldots \oplus M'_t$ for which either M'_j is a term in $sat(\Gamma)$ or M'_j is a subterm of a term in $sat(\Gamma)$ $(1 \leq j \leq t)$. It might be the case that R is empty.

Induction Basis. Suppose that there exists only one occurrence of $\oplus$ in C_{M_0}.

Then, $C_{M_0} = C_{M_{01}}[x_1, \ldots, x_m] \oplus C_{M_{02}}[x_{m+1}, \ldots, x_{k_0}]$.

Hence, $C[T_1, \ldots, T_k]|_p = C'_1[T_{1_1}, \ldots, T_{1_{r_1}}] \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$ for contexts C'_1 and C'_2 and terms $T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$.

- $|C'_1| > 1$ and $|C'_2| > 1$
  Note that since C'_1 are C'_2 headed with function symbols different from $\oplus$ then the result follows for $r = 2$ and terms M' and M'' empty in (A.1). That is, $C[T_1, \ldots, T_k] =_{AC} C^*[\ldots, \underbrace{\bigoplus_{i=1}^{2} C'_i[T_{i_1}, \ldots, Ti_{r_i}]}_{\text{position } -p}, \ldots]$ for some context C^* with $pn(C^*) \cap \tilde{n} = \emptyset$. In this case $C[T_1, \ldots, T_k]|_p$ is in case a).
- $C'_1 = \Box$ and $|C'_2| > 1$.
  Suppose that there is a position $q \in \mathcal{P}os(C[T_1, \ldots, T_k])$ such that $C[T_1, \ldots, T_k]|_q = T_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$, for some context C'_2 such that $C'_2|_\varepsilon \neq \oplus$ and terms $T_u, T_{2_1}, \ldots, T_{2_{r_2}} \in \{T_1, \ldots, T_k\}$ and $T_u = T'_u \oplus T''_u$.

$$\begin{aligned} &C[T_1, \ldots, T_k]|_q = T_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}] = (T'_u \oplus T''_u) \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}] \\ &=_{AC} T''_u \oplus \underbrace{T'_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]}_{=_{AC} M_0\theta} \end{aligned} \tag{A.2}$$

  In this case $C[T_1, \ldots, T_k]|_p$ is in case b) for some position $p \in \mathcal{P}os(C[T_1, \ldots, T_k])$ such that $C[T_1, \ldots, T_k]|_p = T'_u \oplus C'_2[T_{2_1}, \ldots, T_{2_{r_2}}]$.

Induction Step. Suppose that there exist n occurrences of $\oplus$ in C_{M_0}.

Then, $C_{M_0} = C_{M_{01}}[x_1, \ldots, x_m] \oplus C_{M_{02}}[x_{m+1}, \ldots, x_{k_0}]$ for contexts $C_{M_{01}}$ and $C_{M_{02}}$ that have a number of occurrences of $\oplus$ smaller than n.

Case 1. $|C_{M_{01}}| = 1$ and $|C_{M_{02}}| > 1$.

ACCEPTED MANUSCRIPT

In this case, $C_{M01} = \Box$ and the overall structure of C_{M_0} is: $C_{M_0}[x_1, \ldots, x_{k_0}] = x_1 \oplus C_{M_{02}}[x_2, \ldots, x_{k_0}]$. Suppose that $C[T_1, \ldots, T_k]|_p = C_1[T_{11}, \ldots, T_{1_{r1}}] \oplus C_2[T_{21}, \ldots, T_{2_{r2}}]$ and that

- $C_1[T_{11}, \ldots, T_{1_{r1}}] =_{AC} x_1\theta$; and
- $C_2[T_{21}, \ldots, T_{2_{r2}}] =_{AC} C_{M_{02}}[x_2, \ldots, x_{k_0}]$

for some substitution θ.

By induction hypothesis, $C_2[T_{21}, \ldots, T_{2_{r2}}] =_{AC} R_2 \oplus \bigoplus_{i=1}^{s_0} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]$.

i. $C_1|_\varepsilon = \Box$.
Then $r_1 = 1$ and $C_1[T_{11}, \ldots, T_{1_{r1}}] =_{AC} = T_{11}$. In this case, either $T_{11} \in sat(\Gamma)$ or T_{11} is a subterm of a term in $sat(\Gamma)$. For the second case, there exist $q \in \mathcal{P}os(C[T_1, \ldots, T_k])$ and a term $T_{11} \oplus T_{21} \in$ such that

$$C[T_1, \ldots, T_k]|_q = (T_{11} \oplus T_{21}) \oplus C_2[T_{21}, \ldots, T_{2_{r2}}] =_{AC} T_{21} \oplus \underbrace{T_{11} \oplus C_2[T_{21}, \ldots, T_{2_{r2}}]}_{C[T_1, \ldots, T_k]|_p}$$

ii. $C_1|_\varepsilon = f$, $f \in \Sigma_E$ and $f \neq \oplus$.
Then, $C[T_1, \ldots, T_k]|_p =_{AC} R_2 \oplus C_1[T_{11}, \ldots, T_{1_{r1}}] \oplus \bigoplus_{i=1}^{s_0} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]$ and result follows.

iii. $C_1|_\varepsilon = \oplus$.
In this case, $C_1[T_{11}, \ldots, T_{1_{r1}}] = T'_1 \oplus \ldots \oplus T'_m \oplus \bigoplus_{j=1}^{s_1} C'_j[T_{j_1}, \ldots, T_{j_{r_j}}]$ where each T'_i is either in or is a subterm of , C'_j is a context not headed with $\oplus$ and $T_{j_1}, \ldots, T_{j_{r_j}} \in \{T_1 \ldots, T_k\}$ $(1 \leq j \leq s_1$ and $1 \leq i \leq m)$. Therefore,

$$C[T_1, \ldots, T_k]|_p =_{AC} T'_1 \oplus \ldots \oplus T'_m \oplus \bigoplus_{j_1}^{s_1} C'_j[T_{j_1}, \ldots, T_{j_{r_j}}] \oplus R_2 \oplus \bigoplus_{i=1}^{s_0} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]$$

$$=_{AC} R \oplus \bigoplus_{j=1}^{s_1} C'_j[T_{j_1}, \ldots, T_{j_{r_j}}] \oplus \bigoplus_{i=1}^{s_0} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]$$

for $R = T'_1 \oplus \ldots \oplus T'_m \oplus R_2$ and result follows.

Case 2. $|C_{M_{01}}| > 1$ and $|C_{M_{02}}| > 1$.
In this case, one has to apply the induction hypothesis and the result follows.

□

The following proposition establishes a structural classification of the instances of the variables of the (lhs) of a rule $M_0 \to N_0$ occurring in the term $C[T_1, \ldots, T_k]$ which is reducible by this rule. This proposition was partially stated in the proof of Lemma 11 [1], here we present two new cases which an occurrence of a variable could satisfy. We assume that the contexts used in Proposition 32 do not contain private names ($pn(C) \cap \tilde{n} = \emptyset$).

Proposition 32 (Classification)**.** *Let E be an $\mathbf{N}$-locally stable equational theory. Suppose that $C[T_1, \ldots, T_k] \to_{AC} T$, for a minimal context C and terms $T_1, \ldots, T_k \in S$. By Lemma 31, $C[T_1, \ldots, T_k] =_{AC} C'[M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}], T_1, \ldots, T_k]$, for some context C' . For each i, $C'_i|_\epsilon \neq \oplus$, $C'_i \neq \Box$, $T_{i_1}, \ldots, T_{i_{s_i}} \in sat(\Gamma)$, where $M' = M'_1 \oplus \ldots \oplus M'_l$, $M'' = M''_1 \oplus \ldots \oplus M''_l$*

ACCEPTED MANUSCRIPT

with $M'_j \oplus M''_j \in sat(\Gamma)$[12]. *Then, there exist a subterm* A *of* $C[T_1, \ldots, T_k]$ *such that* $A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$(for some $r' \in \mathbb{N}, 1 \leq r' \leq r$) *is an instance* $M_0\theta$ *(modulo AC) of the (lhs) of some rule* $M_0 \to N_0 \in \mathcal{R}_E$.

For each variable x *in* M_0*, consider the occurrences of* $x\theta$ *in* A. *Then*

1. $x\theta$ *occurs as a subterm of* M'_j *for some index* $j = 1, \ldots, l$;
2. *or* $M' =_{AC} x\theta \oplus R$, *for some term* R *which will be matched with other instances of variables in* $\mathcal{V}ar(M_0)$;
3. *or* $x\theta$ *occurs as a subterm of* T_{i_j} *for some* i *and some* j;
4. *or* $x\theta =_{AC} C''[T'_1, \ldots, T'_s]$ *for some context* C'' *that satisfies Lemma 30 (i.e.,* $C'' \neq \Box$*) and* $T'_1, \ldots, T'_s \in \{T_1, \ldots, T_k\} \in sat(\Gamma)$ *such that* $C''[T'_1, \ldots, T'_s]$ *is a subterm of* $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$, *for some* $s \in \mathbb{N}$;
5. *or* $x\theta =_{AC} R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ *for some subterm* R *(which can be empty) of* M' *and some* $k \in \mathbb{N}$, *such that* $1 \leq k \leq r'$.

Proof. By the Structural Characterisation of Redexes Lemma (Lemma 31) one has that

$$C[T_1, \ldots, T_k] =_{AC} C^*[T_{j_1}, \ldots, T_{j_s}, \underbrace{M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{r_i}}]}_{\text{position } q}, T_{j_{s+1}} \ldots, T_{j_w}]$$

where C'_i and C^* are contexts, $1 \leq i \leq r$ for some $r \in \mathbb{N}$ and some position q of $C[T_1, \ldots, T_k]$. In addition to this, $M' = M'_1 \oplus \ldots \oplus M'_t$, $M'' = M''_1 \oplus \ldots \oplus M''_l$ for some $, t, l \in \mathbb{N}$ ($t \leq l$) such that $M'_u \oplus M''_u \in sat(\Gamma)$, $1 \leq u \leq l$. For $1 \leq i \leq r$ one has that $C'_i|_\varepsilon \neq \oplus$ and $T_{j_1}, \ldots, T_{j_w}, T_{i_1}, \ldots, T_{i_{r_i}} \in \{T_1, \ldots, T_k\}$.

Assume, without loss of generality, that the terms in $sat(\Gamma)$ are in normal form (by Definition 12, for each $M \in sat(\Gamma)$, it follows that $M{\downarrow} \in sat(\Gamma)$).

Suppose that the rule $M_0 \to N_0$ applied in A has the following form: $C_{M_0}[x_1, \ldots, x_{k_0}] \to C_{N_0}[x_1, \ldots, x_{k'_0}]$. for contexts C_{M_0} and C_{N_0} whose holes were instantiated with the variables $x_1 \ldots x_{k_0} \in \mathcal{V}ar(M_0)$ that may occur more than once in M_0 (M_0 and N_0 may not be linear), for some $k_0 \in \mathbb{N}$. That is, C_{M_0} is the context of the term M_0, whose holes are in the positions of the variables of M_0. In order to have an instance $M_0\theta$ of M_0 it is necessary to keep the correspondence between the holes of the same variables. Taking this into account, consider that $A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$, for some substitution θ.

The proof follows by induction on the number of occurrences of $\oplus$ in C_{M_0}.

Base Case $n = 0$

There are no occurrences of $\oplus$ in C_{M_0}. This case will be split in the following subcases:

[12] $r \in \mathbb{N}, i = 1, \ldots, r\,, i_j \in \{1, \ldots, k\}, l \in \mathbb{N}$ and $1 \leq j \leq l$

ACCEPTED MANUSCRIPT

0.a) $l > 0$ and $r' = 0$

That is,

$$A \stackrel{def}{=} M' =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta] \tag{A.3}$$

where C_{M_0} does not contain instances of $\oplus$.

For each occurrence of $x \in \mathcal{V}ar(M_0)$ in A, $x\theta$ occurs as a subterm of M'. The following subcases will be analysed:

- either $x\theta$ occurs as a subterm of M'_i, for some index $i = 1, \ldots, l$.
  By equation A.3, it follows that parts of the term M' should be matched with some part of $C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$.
  When $l > 1$ it is necessary that other variables of M_0, when instantiated with θ, match the remaining part of M'. Since, by hypothesis, $M' = M_1 \oplus \ldots \oplus M'_l$, it would be necessary the occurrence of at least one $\oplus$ em C_{M_0}. Contradiction.
  When $l = 1$, it follows that each occurrence of one variable x in M_0 is an instance of a subterm of M'_1. And the reduction would happen in M'_1. By hypothesis, one has that $M'_1 \oplus M''_1 \in sat(\Gamma)$, therefore, M'_1 is in normal form. Contradiction.
- or $M' =_{AC} x\theta \oplus R$, for some term R.
  Since $M' =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$, it follows that the subterm R in M' matches instances of variables from M_0 via θ. However, if there exist at least one occurrence of a variable $y \in \mathcal{V}ar(M_0)$ such that $y\theta = R$, one has: $M' = x\theta \oplus y\theta$, and then, C_{M_0} would contain an instance of $\oplus$. Contradiction.

0.b) $l = 0$ and $r' > 0$

That is, $A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$, with $C'_i|_\varepsilon \neq \oplus$ and $C'_i \neq \Box$, for all $i = 1, \ldots, r'$. Notice that this case happens only when $r' = 1$. Otherwise, occurrences of $\oplus$ in C_{M_0} would be necessary.

Suppose that $r' = 1$. Then, $C[T_{1_1}, \ldots, T_{1_{s_1}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$. For each occurrence of $x \in \mathcal{V}ar(M_0)$ in A, it follows that: either $x\theta$ occurs as a subterm of T_{1_j}, for some $j = 1, \ldots, s_1$; or $x\theta = C''_1[T'_1, \ldots, T'_s]$ for some subterm $C''_1[T'_1, \ldots, T'_s]$ of $C'_1[T_{1_1}, \ldots, T_{1_{s_1}}]$.

0.c) $l > 0$ and $r' > 0$

That is, $A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_0}[x_1\theta, \ldots, x_{k_0}\theta]$, where $C'_i|_\varepsilon \neq \oplus$ and $C'_i \neq \Box$, for $i = 1, \ldots, r'$. In this case, at least one occurrence of $\oplus$ in C_{M_0} is necessary. This case does not happen.

Induction Step. Suppose that C_{M_0} contains n occurrences of $\oplus$. That is, $C_{M_0}[x_1, \ldots, x_{k_0}] = C'_{M_0}[C_{M01}[x_1, \ldots, x_u] \oplus C_{M02}[x_{u+1}, \ldots, x_{k_0}]]$, for some context C'_{M_0} that does not contain occurrence of $\oplus$, and contexts C_{M01} and C_{M02} such that #{occurrences of $\oplus$in C_{M01}}$\cup$#{occurrences of $\oplus$ inC_{M02}} $\leq n - 1$. This case will be divided in the following subcases:

1. $C'_{M_0}|_\varepsilon = f$, $f \neq \oplus$.

ACCEPTED MANUSCRIPT

1.1 $l > 0$ and $r' = 0$, that is, M_0 is not headed with $\oplus$;

Then, $A \stackrel{def}{=} M' =_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]]$ The only possible case happens when $l = 1$ and then the reduction would happen in M'_1. At the same time, $M'_1 \oplus M''_1 \in sat(\Gamma)$ wherefore, M'_1 is in normal form. Contradiction.

1.2 $l = 0$ and $r' > 0$;

Then, $A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]]$.

Since $C'_{M_0}|_\varepsilon \neq \oplus$, the only possible case happens when $r' = 1$. Thus, for each $x \in \mathcal{V}ar(M_0)$, it follows that: $x\theta$ occurs as in case 1 or case 4. And the result follows.

1.3 $l > 0$ and $r' > 0$. In this case, $A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C'_{M_0}[C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]]$. Since $C'_{M_0}|_\varepsilon \neq \oplus$, this case is not possible.

2. $C'_{M_0} = \Box$, that is, M_0 is headed with $\oplus$.

Then, $C_{M_0}[x_1, \ldots, x_{k_0}] = C_{M01}[x_1, \ldots, x_u] \oplus C_{M02}[x_{u+1}, \ldots, x_{k_0}]$. The analysis will be divided in the following subcases:

2.1) $l > 0$ and $r' = 0$.

Then, $A \stackrel{def}{=} M'_1 \oplus \ldots \oplus M'_l =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta] \oplus C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$. Suppose that the occurrence of $\oplus$ which is explicit in C_{M_0} matches with an occurrence of $\oplus$ in A in the following way: $M'_1 \oplus \ldots \oplus M'_k =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta]$ and $M'_{k+1} \oplus \ldots \oplus M'_l =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$, with $1 \leq k \leq l$. Since C_{M01} and C_{M02} are contexts with a number $< n$ of occurrences of $\oplus$ in its composition, the result follows by induction hypothesis.

Suppose that the occurrence of $\oplus$ that is explicit in C_{M_0} matches with an occurrence of $\oplus$ of A in the following way: $u_1 \oplus \ldots \oplus u_q =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta]$ and $M^*_1 \oplus \ldots \oplus M^*_q \oplus M'_{q+1} \ldots \oplus M'_l =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$. where $M'_j = u_j \oplus M^*_j$ for $1 \leq j \leq q \leq l$. And the result follows by induction hypothesis.

2.2) $l = 0$ and $r' > 0$.

Then $A \stackrel{def}{=} \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$.

This case happens only when the occurrence of $\oplus$ that is explicit in C_{M_0} matches with the j-th occurrence of $\oplus$ in A, for some $j \in \mathbb{N}$, $1 \leq j \leq r'$. That is,

$$\bigoplus_{i=1}^{j} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M01}[x_1\theta, \ldots, x_u\theta] \qquad \bigoplus_{i=j+1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M02}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$$

and the result follows by induction hypothesis.

2.3) $l > 0$ and $r' > 0$.

Then, $A \stackrel{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta] \oplus C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$. The following possibilities have to be analysed:

- $M' =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ and $\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$.

ACCEPTED MANUSCRIPT

- $M' =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ and $R_2 \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$, for subterms R_1 and R_2 of M' such that $M' =_{AC} R_1 \oplus R_2$.
- $R_1 \bigoplus_{i=1}^{m} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{01}}[x_1\theta, \ldots, x_u\theta]$ and $R_2 \bigoplus_{i=m+1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C_{M_{02}}[x_{u+1}\theta, \ldots, x_{k_0}\theta]$ for subterms R_1 and R_2 of M' such that $M' =_{AC} R_1 \oplus R_2$ and some $s \in \mathbb{N}$, with $m \leq r'$.

In all the cases the result follows by induction hypothesis.

□

Example 11. Consider the case where $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] = g(f(T_{i_1}, T_{i_2}, T_{i_3}), T_{i_4})$, where $C'_i[\_] = g(f(\_, \_, \_), \_)$, $f, g \in \Sigma_E$, $f \neq \oplus$ and $g \neq \oplus$. The case in which $x\theta = f(T_{i_1}, T_{i_2}, T_{i_3})$ is an example of an instance of variable x being in case 4. The case in which $y\theta = T'_{i_4}$, where $T_{i_4} = h(T'_{i_4})$ (for some $h \in \Sigma_E$) is an example of a variable y being in case 3[13].

Proposition 33. . *The case 5 of Proposition 32 does not occur simultaneously with cases 1, 2 ou 3 for the same variable x.*

Proof. The proof follows by the analysis of each possible case.

- If case 5 were to occur simultaneously with case 1 (or case 3) for the same variable x, then $x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ would be a subterm of T_i or M'_i.

  Suppose that $x\theta$ is subterm of M'_i, for some index i. Then, $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \in st_E(M'_i) \subseteq st_E(M'_i \oplus M''_i) \subseteq st_E()$, since $M'_i \oplus M''_i \in sat(\Gamma)$. Therefore, by item 2 of Definition 12, one has $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] = T \in sat(\Gamma)$ contradicting the fact that the context C' satisfies Lemma 30 (i.e., $C'_i| \neq \Box$) for each $i = 1, \ldots, k$. The analysis is similar when $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \in st_E(T_i)$
- If case 5 were to occur simultaneously with case 2 for the same variable x.

  On one hand, $x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ for a subterm R of M'. On the other hand, $M' = x\theta \oplus R_1$. for some subterm R_1 of M'. Then $M' =_{AC} R \oplus C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus R_1$. Since, for each $i = 1, \ldots, k$, $C'_i|_\varepsilon \neq \oplus$ and $C'_i \neq \Box$, one has that $C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ is a subterm of M'_j, for some $1 \leq j \leq l$, and the contradiction follows similarly to the previous case.

□

Proposition 34. *The case 4 of Proposition 32 does not occur simultaneously with cases 1, 2 or 3.*

Proof. The proof is done by analysing the cases: When case 4 occurs simultaneously with case 1 or 3 for the same variable $x \in \mathcal{V}ar(M_0)$ the analysis is similar to the proof the the previous lemma; When case 4 occurs simultaneously with case 2 the contradiction follows from the fact that C'' satisfies Lemma 30. □

[13] These cases were not considered in Lemma 11 [1]

ACCEPTED MANUSCRIPT

Remark 7. [Justification] Notice what happens when case 5 of Proposition 32 occurs simultaneously with case 4 for an occurrence of the same variable x:

On one hand, $x\theta = R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$, for some subterm R (which may be empty) of M' and some $k \in \mathbb{N}$, such that $1 \leq k \leq r'$. On the other hand, $x\theta =_{AC} C''[T'_1, \ldots, T'_s]$, for some context C'' that satisfies the Lemma 30 (that is, $C'' \neq \Box$) and subterms $T'_1, \ldots, T'_s$ of the terms $T_1, \ldots, T_k \in sat(\Gamma)$ such that $C''[T'_1, \ldots, T'_s]$ is subterm of $C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]$, for some $j \in \mathbb{N}$, $1 \leq j \leq r'$. Therefore, $R \oplus \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] =_{AC} C''[T'_1, \ldots, T'_s] =_{AC} C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]|_q$. for some position $q \neq \varepsilon$.

By hypothesis, $T'_1, \ldots, T'_s$ are subterms of the terms $T_1, \ldots, T_k \in sat(\Gamma)$, the only way to split the terms $T_1, \ldots, T_k \in sat(\Gamma)$ in "independent subterms" happens when this term is headed with $\oplus$. That is, there exists at least one term $T_n = u_n \oplus v_n$, for some index $n \in \mathbb{N}$ and subterms u_n and v_n such that the context C'_j has the following form:

$$\begin{aligned} C'_j[T_{j_1}, \ldots, T_n, \ldots, T_{j_{s_j}}] &=_{AC} C''_j[C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus T_n, \ldots, T_]\\ &=_{AC} C''_j[C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus (u_n \oplus v_n), \ldots, T_{j_{s_j}}]\\ &=_{AC} C''_j[\underbrace{(C^*_j[T_{j_1}, \ldots, T_{n-1}, T_{n+1}, \ldots, T_s] \oplus u_n)}_{C'_j[T_{j_1}, \ldots, T_{j_{s_j}}]|_q} \oplus v_n, \ldots, T_{j_{s_j}}] \end{aligned}$$

Lemma (Lifting) *Let E be an $\mathbf{N}$-locally stable theory and $\Gamma = \{M_1, \ldots, M_n\}$ a set of ground terms in normal form. For every context C_1, for every $T_1, \ldots, T_k \in sat(\Gamma)$, for every term T such that $C_1[T_1, \ldots, T_k] \to_{\mathcal{R} \cup AC} T$, there exists an AC-normal context C_2, and terms $T'_1, \ldots, T'_l \in sat(\Gamma)$, such that $T \overset{*}{\to}_{\mathcal{R} \cup AC} C_2[T'_1, \ldots, T'_l]$.*

Proof. Suppose that $C_1[T_1, \ldots, T_k] \to_{AC} T$, for a normal context C_1 and terms $T_1, \ldots, T_k \in sat(\Gamma)$. Notice that, since E is AC-convergent, every context can be normalised. From Proposition 32 it follows that: $C_1[T_1, \ldots, T_k] = C'[M'' \oplus M' \oplus \bigoplus_{i=1}^{r} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}], T_1, \ldots, T_k]$, for some context C' and $r \in \mathbb{N}$. For each $i = 1, \ldots, r$, $C'_i|_\epsilon \neq \oplus$, $C'_i \neq \Box$, $T_{i_1}, \ldots, T_{i_{s_i}} \in sat(\Gamma)$, $i_j \in \{1, \ldots, k\}$, the terms M' and M'' are such that $M' = M'_1 \oplus \ldots \oplus M'_l$, $M'' = M''_1 \oplus \ldots \oplus M''_l$ with $M'_j \oplus M''_j \in sat(\Gamma)$, where $l \in \mathbb{N}$ and $1 \leq j \leq l$. Then, there exists a subterm A of $C[T_1, \ldots, T_k]$ such that $A \overset{def}{=} M' \oplus \bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ (for some $r' \in \mathbb{N}, 1 \leq r' \leq r$) is an instance $M_0\theta$ (modulo AC) the (lhs) of some rule $M_0 \to N_0 \in \mathcal{R}_E$. For each $x \in \mathcal{V}ar(M_0)$ one has that $x\theta$ occurs as in the cases 1, 2, 3, 4 or 5 of Proposition 32, for some substitution θ.

Since for every $T \in sat(\Gamma)$, $T\downarrow \in sat(\Gamma)$ one can assume, without loss of generality, that all the terms $T_1, \ldots, T_k$ in $sat(\Gamma)$ are in normal form. Therefore, the reduction cannot occur inside the terms T_i, $1 \leq i \leq k$.

Without loss of generality, suppose that the variables of M_0 are $x_1, \ldots, x_{k_1}, y_1, \ldots, y_{k_2}, z_1, \ldots, z_{k_3}$, where x_i's are in the cases 1, 2 or 3, z_r's are in the case 4 which do not occur simultaneously with case 5, and y_j's are in case 5 or case 4 which occur simultaneously with case 5.

For each variable y_j, consider the l (for some $l \in \mathbb{N}$) occurrences of $y_j\theta$ in A:

$$y_j\theta =_{AC} R^1_j \oplus \bigoplus_{i=1}^{k} C^j_{1i}[T^1_{i_1}, \ldots, T^1_{i_{s_i}}](\text{ 1st occurrence})$$

$$=_{AC} R^2_j \oplus \bigoplus_{i=1}^{k} C^j_{2i}[T^2_{i_1}, \ldots, T^2_{i_{s_i}}](\text{ 2nd occurrence}) =_{AC} \ldots =_{AC} R^l_j \oplus \bigoplus_{i=1}^{k} C^j_{li}[T^l_{i_1}, \ldots, T^l_{i_{s_i}}](\text{ l}th\text{ occurrence})$$

ACCEPTED MANUSCRIPT

where for each u, $1 \leq u \leq l$, R^u_j is subterm of M', and each context $C^j_{u_i}$ are such that $C^j_{u_i}|_\varepsilon \neq \oplus$ and $C^j_{u_i} \neq \Box$. The superscripts on the terms $T_{i_1}, \ldots, T_{i_{s_i}} \in sat(\Gamma)$ indicate the number of the occurrence that each one of the terms occur.

For each i, denote with $cl(C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}])$ the class of $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ modulo AC, and associate with a fresh name $a_{cl(C^j_{ui}[T^u_{i_1},\ldots,T^u_{i_{s_i}}])}$ each class $cl(C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}])$, $1 \leq u \leq l$. Then, $a_{cl(C^j_{ui}[T^u_{i_1},\ldots,T^u_{i_{s_i}}])} = a_{cl(C^j_{vi}[T^v_{i_1},\ldots,T^v_{i_{s_i}}])}$ whenever $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]) =_{AC} C^j_{vi}[T^v_{i_1}, \ldots, T^v_{i_{s_i}}])$, for some $1 \leq v \leq l$.

In each equation $R^u_j \oplus \bigoplus_{i=1}^k C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}] =_{AC} R^v_j \oplus \bigoplus_{i=1}^k C^j_{vi}[T^v_{i_1}, \ldots, T^v_{i_{s_i}}]$, each $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ should be equal modulo AC to one of the $C^j_{vi}[T^v_{i_1}, \ldots, T^v_{i_{s_i}}]$.

If some $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ were equal to some subterm of R^v (for some v), then $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ would be a term of $sat(\Gamma)$, contradicting Lemma 30. Thus,

$$R^1_j \oplus \bigoplus_{i=1}^k a_{cl(C^j_{1i}[T^1_{i_1},\ldots,T^1_{i_{s_i}}])} =_{AC} R^2_j \oplus \bigoplus_{i=1}^k a_{cl(C^j_{2i}[T^2_{i_1},\ldots,T^2_{i_{s_i}}])} =_{AC} \quad \ldots \quad =_{AC} R^l_j \oplus \bigoplus_{i=1}^k a_{cl(C^j_{li}[T^l_{i_1},\ldots,T^l_{i_{s_i}}])} \stackrel{def}{=} T_{y_j}.$$

For each variable z_t ($1 \leq t \leq k_3$) consider the $m \in \mathbb{N}$ occurrences of z_t in A:

$$z_t\theta =_{AC} \underbrace{C''_{t_1}[T^1_1, \ldots, T^1_r]}_{\text{1st occurrene}} =_{AC} \ldots =_{AC} \underbrace{C''_{t_m}[T^m_1, \ldots, T^m_r]}_{m\text{−th occurrence}}.$$

Notice that the subscript $w \in \{1, \ldots, m\}$ represents the occurrence of z_t in A. For each w, the context C''_{t_w} and the terms $T^w_1, \ldots, T^w_r$ satisfy the conditions of case 4 of Proposition 32. Similarly to the previous case, write $cl(C''_{t_w}[T^w_1, \ldots, T^w_r])$ for the class $C''_{t_w}[T^w_1, \ldots, T^w_r]$ modulo AC, and associate a fresh name $b_{cl(C''_t[T_1,\ldots,T_r]))}$ with each class. Thus, $z_t\theta =_{AC} b_{cl(C''_t[T_1,\ldots,T_r])}$.

Let θ' be a substitution such that: $x_i\theta' = x_i\theta$, $y_j\theta' = T_{y_j}$ and $z_t\theta' = b_{cl(C''_t[T_1,\ldots,T_r])}$. Let T_2 be the term obtained from $\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}]$ by replacing each $C^j_{ui}[T^u_{i_1}, \ldots, T^u_{i_{s_i}}]$ with $a_{cl(C^j_{ui}[T^u_{i_1},\ldots,T^u_{i_{s_i}}])}$ and each $C''_{t_w}[T^w_1, \ldots, T^w_r]$ with $b_{cl(C''_t[T_1,\ldots,T_r])}$:

$$\begin{aligned}
&\bigoplus_{i=1}^{r'} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] = C'_1[T_{1_1}, \ldots, T_{1_{s_1}}] \oplus \ldots \oplus C'_{r'}[T_{r'_1}, \ldots, T_{r'_{s_{r'}}}] \\
&=_{AC} \bigoplus_{i=1}^{k} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus \bigoplus_{u=k+1}^{r'} \underbrace{C''_u[T_{u_1}, \ldots, T_{u_{s_u}}]}_{\text{instances of } z} \\
&=_{AC} \bigoplus_{i=1}^{m} C'_i[T_{i_1}, \ldots, T_{i_{s_i}}] \oplus \bigoplus_{u=m+1}^{k} a_{cl(C'_u[T_{u_1},\ldots,T_{u_{s_u}}])} \oplus \bigoplus_{u=k+1}^{r'} b_{cl(C''_t[T_1,\ldots,T_r])} \\
&= \ldots = C_2[S_1, \ldots, S_n] \oplus S'_a \oplus S_b = C_3[S_1, \ldots, S_n, S'_a] == T_2
\end{aligned}$$

for some $S_1, \ldots, S_n, S'_a \in sum_\oplus(sat(\Gamma), \tilde{n})$ and $|C_3| \leq |C_{M_0}|$.

On one hand, $A = M' \oplus \bigoplus_{i=1}^r C'_i[T_1, \ldots, T_k] =_{AC} M_0\theta$. On the other hand, $M' \oplus T_2$ is an instance $M_0\theta'$ of M_0. Therefore, $M' \oplus M'' \oplus T_2 \stackrel{h}{\to} M'' \oplus N_0\theta'$ where $M' \oplus M'' =_{AC} \bigoplus_{i=1}^l M'_i \oplus M''_i = S'$, for some $S' \in sum_\oplus(sat(\Gamma), \tilde{n})$, since $M'_i \oplus M''_i \in sat(\Gamma)$, for $1 \leq i \leq l$.

Hence, $M' \oplus M'' \oplus T_2 =_{AC} S' \oplus C_3[S_1, \ldots, S_n, S'_a] = C_4[S', S_1, \ldots, S_n, S'_a] \stackrel{h}{\to}_{AC} M'' \oplus N_0\theta'$. Notice that, since C_4 is a context normal, it follows that $|C_4| = |C_{M_0}| \leq c_E$, by applying rule 3 of Definition 12 the result follows. □

ACCEPTED MANUSCRIPT

Appendix B. Proofs of Section 6

Proof of Proposition 19

Proof. By induction on the structure of the E_{AG}-context, one can prove that :

"if $C[S_1,\ldots,S_l] \xrightarrow{h} M$, where C is a normal E_{AG}-context such that $|C| \leq c_{E_{AG}}$, and where $S_1,\ldots,S_l \in sum_+(,\tilde{n})$, for an AC-symbol $+$, then there exist an E_{AG}-context C', a term M', and terms $S'_1,\ldots,S'_k \in sum_+(sat(\Gamma),\tilde{n})$, such that $M \xrightarrow{*}_{\mathcal{R}\cup AC} M' =_{AC} C'[S'_1,\ldots,S'_k]$"

Base Case $C[\_] = \_$ is the empty E_{AG}-context.

It follows that $l = 1$ and $C[S_1] = S_1 \xrightarrow{h} M$ where $S_1 \in sum_+(sat(\Gamma))$, that is,

$$S_1 = \alpha_1 T_1 + \ldots + \alpha_n T_n + \underbrace{\sum_{j=1}^{r} \beta_j n_j}_{A}, \tag{B.1}$$

for $\alpha_i,\beta_j \in \mathbb{N}^*$, $T_i \in sat(\Gamma)$ and $n_j \notin \tilde{n}$ ($1 \leq i \leq n$ and $1 \leq j \leq r$). The proof follows by analysis of the rewrite rule from $\mathcal{R}_n$ applied in (B.1).

Notice that, in this case, the rule $i(x+y) \to i(x) + i(y)$ could only be applied in some $T_i \in sat(\Gamma)$, by hypothesis, the terms in $sat(\Gamma)$ are in normal form. Therefore, it is necessary to analyse only the applications in S_1 of the following rules:

1. The rule is $x + i(x) \to 0$;

   For this case one has to observe that $C[S_1] = S_1 = \alpha_1 T_1 + \ldots + \alpha_n T_n$ for $\alpha_i \in \mathbb{N}$ and $T_i \in sat(\Gamma)$, is a combination of terms in K_Γ, and the result follows easily.

2. The rule is $x + 0 \to x$;

   Suppose that $T_i = 0$ for some index i in (B.1). The result follows straightforwardly.

Induction Step: One has to analyse normal E_{AG}-contexts C such that $1 \leq |C| \leq c_{E_{AG}}$.
The following E_{AG}-contexts will be analysed:

1. $C[\_] = i(\_)$

   In this case one has $C[S_1] = i(S_1) \xrightarrow{h} M$ and either rule $i(i(x)) \to x$ or rule $i(x+y) \to i(x) + i(y)$ can be applied.

   - the rule $i(i(x)) \to$ is applied.

     Then, $S_1 = T_1 = i(T'_1)$ where $T_i \in sat(\Gamma)$. Therefore, $C[S_1] = i(i(T'_1)) \xrightarrow{h} T'_1 \in sat(\Gamma)$ by rule 4 of the definition of $sat(\Gamma)$ for Abelian Groups. The result follows for an empty E_{AG}-context.
   - the rule $i(x+y) \to i(x) + i(y)$ is applied. In this case, $C[S_1] = i(\alpha_1 T_1 + \ldots + \alpha_n T_n + \underbrace{\sum_{j=1}^{r} \beta_j n_j}_{A})$ for $\alpha_i,\beta_j \in \mathbb{N}^*$, $T_i \in sat(\Gamma)$ and $n_j \notin \tilde{n}$ ($1 \leq i \leq n$ and $1 \leq j \leq r$). Using the AC properties, it follows that

$$C[S_1] = i(\alpha_1 T_1 + \ldots + \alpha_n T_n + A) = i(T_1 + (\alpha_1 - 1)T_1 + \ldots + \alpha_n T_n + A)$$
$$\xrightarrow{h} i(T_1) + i((\alpha_1 - 1)T_1 + \ldots + \alpha_n T_n + A) = M$$

ACCEPTED MANUSCRIPT

Proceeding analogously, it follows that $M \xrightarrow{*} \alpha_1 i(T_1)\downarrow + \alpha_2 i(T_2)\downarrow + \ldots + i(\alpha_n T_n + A)$. Since $T_i \in sat(\Gamma)$ for $1 \leq i \leq n$, it follows by definition of $sat(\Gamma)$ for Abelian Groups that $i(T_i)\downarrow \in$. Therefore, the result follows for the context $C[] = \_ + i(\_)$.

2. $C[\_] = \_ + \_$
   In this case, one has
   $$C[S_1, \ldots, S_k] = S_1 + \ldots + S_k \tag{B.2}$$
   where $S_1, \ldots, S_k \in sum_+(sat(\Gamma), \tilde{n})$. Reorganising the repeated terms from $sat(\Gamma)$ in (B.2), one has that $C[S_1, \ldots, S_k] = S_1 + \ldots + S_k =_{AC} S' \in sum_+(sat(\Gamma), \tilde{n})$, and the result follows by the Base Case.

3. $C[\_] = i(\_) + i(\_)$ and $C[\_] = \_ + i(\_)$. These cases are similar to the previous.

□

Appendix C. Proof of Lemma 23

Proof. We want to prove that

"If $C[S_1, \ldots, S_k] \xrightarrow{h} M$ where C is a normal E_{AG^h}-context such that $|C| \leq c_{E^h_{AG}} = 5$ and where $S_1, \ldots, S_k \in sum_\oplus(sat(\Gamma), \tilde{n})$ (for $\oplus \in \{+, \bullet\}$), then there exist a normal context C', a term M' and terms $S'_1, \ldots, S'_r \in sum_\oplus(sat(\Gamma), \tilde{n})$ (for $\oplus \in \{+, \bullet\}$) such that $M \xrightarrow{*} M' =_{AC} C'[S'_1, \ldots, S'_r]$"

The proof is by induction on the structure of the E_{AG^h}-context.

Base Case. $C = \_$, that is, C is the empty E_{AG^h}-context.

Then $k = 1$ and $C[S_1] = S_1 \xrightarrow{h} M$, $S_1 \in sum_\oplus(sat(\Gamma), \tilde{n})$ for $\oplus \in \{+, \cdot\}$.

1. $\oplus = +$

   Then $S_1 = \alpha_1 T_1 + \ldots + \alpha_n T_n + \underbrace{\beta_1 n_1 + \ldots + \beta_r n_r}_{A}$ where $T_i \in sat(\Gamma), n_j \notin \tilde{n}, \alpha_i, \beta_j \in \mathbb{N}$ for $1 \leq i \leq n$ and $1 \leq j \leq r$.

   Notice that, the function symbol $+$ is only applied to exponents (which are integers).

   The analysis follows by examining the rules applied in S_1. Since S_1 is composed of normal terms $T_1, \ldots, T_n$, the possible applicable rules are:

   1.1 The rule is $x + 0 \to x$:

   In this case, there must be an index i such that $T_i = 0$, for $1 \leq i \leq n$. Suppose, without loss of generality that $i = 1$, then

   $$S_1 = \alpha_1 0 + \alpha_2 T_2 + \ldots + \alpha_n T_n + A =_{AC} 0 + ((\alpha_1 - 1)0 + \alpha_2 T_2 + \ldots + \alpha_n T_n + A)$$
   $$\xrightarrow{h} ((\alpha_1 - 1)0 + \alpha_2 T_2 + \ldots + \alpha_n T_n + A) = M.$$

   Repeating the reasoning above, it follows that $M \xrightarrow{*} \alpha_2 T_2 + \ldots + \alpha_n T_n + A = M' =_{AC'} S'_1 \in sum_+(sat(\Gamma), \tilde{n})$, and the result follows for the empty E_{AG^h}-context.

   1.2 $x + i(x) \to 0$

   This case is similar to the proof for Abelian Groups.

ACCEPTED MANUSCRIPT

2. $\oplus = \bullet$.

   Then $S_1 = T_1^{\alpha_1} \cdot \ldots \cdot T_n^{\alpha_n} \cdot \underbrace{n_1^{\beta_1} \cdot \ldots \cdot n_r^{\beta_r}}_{B}$ where $T_i \in sat(\Gamma), n_j \notin \tilde{n}, \alpha_i, \beta_j \in \mathbb{N}$ for $1 \leq i \leq n$ and $1 \leq j \leq r$.

   Remark 8. Notice that the function symbol $\cdot$ (multiplication) is applied in exponentials (elements of the group $\mathbb{Z}_p^*$), products between an element of $\mathbb{Z}_p^*$ and an integer, that is, the case in which the rule $exp(h(x), y) \rightarrow h(x \cdot y)$ has been applied.

   The possible rules that can be applied in S_1 are:

   2.1 $x \cdot 1 \rightarrow x$. This case is similar to case 1.1 above.

   2.2 $h(x) \cdot h(y) \rightarrow h(x + y)$;

   In this case there exist indexes $i, j \in \{1, \ldots, n\}$ such that $T_i = h(T_i') \cdot u_i$, $T_j = h(T_j') \cdot u_j$, where u_i and u_j are possibly empty. Then,

$$S_1 =_{AC} T_1^{\alpha_1} \cdot \ldots \cdot T_i^{\alpha_i} \cdot \ldots \cdot T_j^{\alpha_j} \cdot \ldots \cdot T_n^{\alpha_n} \cdot B =_{AC} (T_i \cdot T_j) \cdot \underbrace{(T_1^{\alpha_1} \cdot \ldots \cdot T_i^{(\alpha_i - 1)} \cdot \ldots \cdot T_j^{(\alpha_j - 1)} \cdot \ldots \cdot T_n^{\alpha_n}) \cdot B}_{T}$$

$$=_{AC} (h(T_i') \cdot u_i \cdot h(T_j') \cdot u_j) \cdot T \overset{h}{\rightarrow} h(T_i' + T_j') \cdot u_i \cdot u_j \cdot T = M$$

   via rule $h(x) \cdot h(y) \rightarrow h(x + y)$.

   Repeating the same reasoning, it follows that $M \overset{*}{\rightarrow} h(\alpha_i T_i' + \alpha_j T_j') \cdot u_i^{\alpha_i} \cdot u_j^{\alpha_j} \cdot T^*$ where $T^* = R_1^{\gamma_1} \cdot \ldots \cdot R_m^{\gamma_m} \cdot B$, where $R_j \in \{T_1, \ldots, T_n\} - \{T_i, T_j\}$ and $\gamma_j = \alpha_j$.

   Since $T_i, T_j \in sat(\Gamma)$ and $T_i \cdot T_j \overset{h}{\rightarrow} h(T_i' + T_j') \cdot u_i \cdot u_j = N$ via rule $h(x) \cdot h(y) \rightarrow h(x + y)$, it follows, by rule 7 of Definition 27 of $sat(\Gamma)$, that $N \downarrow = (h(T_i' + T_j') \cdot u_i \cdot u_j) \downarrow \in sat(\Gamma) \subset sum_\bullet(sat(\Gamma), \tilde{n})$. Therefore, $M \overset{*}{\rightarrow} (h(\alpha_i T_i' + \alpha_j T_j') \cdot u_i^{\alpha_i} \cdot u_j^{\alpha_j}) \downarrow \cdot T^* =_{AC} S' \in sum_\bullet(sat(\Gamma), \tilde{n})$, and the result follows for an empty context.

   2.3 $x \cdot j(x) \rightarrow 1$;

   This case is similar to + AC function symbol, and uses the definition of sets $K_\Gamma^\oplus$ and $A_\Gamma^\oplus$, when $\oplus = \cdot$.

Induction Step. We will analyse the possible normal E_{AG^h}-contexts C such that $|C| \leq c_{E_{AG^h}} = 5$.

1. $C[\_] = i(T[\_])$ for $|T[\_]| \leq 4$. In this case, the proof is similar to the theory of Abelian Groups E_{AG}.

2. $C[\_] = j(T[\_])$ for $|T[\_]| \leq 4$. In this case, we have $C[S_1, \ldots, S_r] = j(C[S_1, \ldots, S_r]) \overset{h}{\rightarrow} M$. For a head reduction one of the following configurations of E_{AG^h}-contexts must happen:

   (a) $T[\_] = j(T'[\_])$ or $T[\_] = h(T'[\_])$ or $T[\_] = T_1[\_] \cdot T_2[\_]$

   Notice that , $C[\_] = j(j(T'[\_])$ or $C[\_] = j(h(T'[\_])$ or $C[\_] = j(T_1[\_] \cdot T_2[\_])$ are not normal E_{AG^h}-contexts, contradicting the hypothesis of the Lemma.

ACCEPTED MANUSCRIPT

(b) $T[\_] = \_$, is the empty context.

In this case, we have $C[S_1] = j(S_1) \xrightarrow{h} M$, and the reduction may happen via an application of rules: $j(h(x)) \to h(i(x))$, or $j(x \cdot y) \to j(x) \cdot j(y)$.

For the first rule, $S_1 = h(T_1)$ where $h(T_1) \in sat(\Gamma)$ is in normal form. Then, $C[S_1] = j(h(T_1)) \xrightarrow{h} h(i(T_1)) = M$. Notice that, there might be a reduction in $i(T_1)$ via application of rule $i(i(x)) \to x$ or $i(x + y) \to i(x) + i(y)$. By Definition 26 it follows that $j(N_1) \downarrow = N \in sat_S(\Gamma)$, for all $N_1 \in sat_S(\Gamma)$. Therefore, $C[S_1] = j(h(T_1)) \xrightarrow{h} h(i(T_1)) \xrightarrow{*} N \in sat_S(\Gamma)$ and the result follows for the empty E_{AG^h}-context $C'[\_] = \_$ and $N \in sum_{\oplus}(sat_S(\Gamma), \tilde{n})$ for $\oplus \in \{+, \cdot\}$.

For the second rule, we would have $S_1 = T_1^{\gamma_1} \cdot T_2^{\gamma_2} \cdot \ldots \cdot T_n^{\gamma_n}$ for $T_j \in sat(\Gamma)$, $\gamma_j, n \in \mathbb{N}$, $1 \leq j \leq n$ for some $n \geq 2$. Then,

$$C[S_1] = j(S_1) = j(T_1^{\gamma_1} \cdot T_2^{\gamma_2} \cdot \ldots \cdot T_n^{\gamma_n}) \xrightarrow{h} j(T_1) \cdot j(T_1^{\gamma_1 - 1} \cdot T_2^{\gamma_2} \cdot \ldots \cdot T_n^{\gamma_n}) = M$$
$$\xrightarrow{*} j(T_1) \downarrow^{\gamma_1} \cdot j(T_2) \downarrow^{\gamma_2} \cdot \ldots \cdot j(T_n) \downarrow^{\gamma_n}) = S' \in sum_{\bullet}(sat(\Gamma), \tilde{n})$$

Since $T_i \in sat(\Gamma)$ it follows that $j(T_i) \downarrow \in sat(\Gamma)$ $(1 \leq i \leq n)$, and the result follows for the empty context.

3. $C[\_] = h(T[\_])$ for $|T[\_]| \leq 4$

   According to the rewriting rules, there is no possible reduction happening in the head of $C[\_]$ unless $C[S_1] = h(0)$, i.e., $C_1 = 0$ and the result is trivial.

4. $C[\_] = exp(C_1[\_], C_2[\_])$ for $|C_1[\_]| + |C_2[\_]| \leq 4$

   That is, $C[S_1, \ldots, S_r] = exp(C_1[S_1, \ldots, S_k], C_2[S_{k+1}, \ldots, S_r]) \xrightarrow{h} M$. This case only happens for $C_1 = \_$ and $S_1 = T_1 = h(T_1') \in sat(\Gamma)$. Therefore,

   $$C[S_1, \ldots, S_r] = exp(S_1, C_2[S_2, \ldots, S_r]) = exp(h(T_1'), C_2[S_2, \ldots, S_r]) \xrightarrow{h} h(T_1' \cdot C_2[S_2, \ldots, S_r]) = M$$

   Notice that $M =_{AC} C'[S_1', \ldots, S_r']$, where $C'[\_] = h(\_ \cdot C_2[\_])$ and $|C'| = |C_2| + 3 \leq 4 - |C_1| + 3 = 7 - |C_1|$, therefore, $4 \leq |C_1| \leq 6$.

5. $C[\_] = C_1[\_] + C_2[\_]$ for $|C_1[\_]| + |C_2[\_]| \leq 4$

   Then, $C[S_1, \ldots, S_k] = C_1[S_1, \ldots, S_q] + C_2[S_{q+1}, \ldots, Sk]$ Since the AC symbols do not distribute over each other, it follows that: if C_i is headed with a function symbol different from + the result follows by I.H.; if C_i is headed with + we split the C_i into sums and repeat the reasoning.

6. $C[\_] = C_1[\_] \cdot C_2[\_]$ for $|C_1[\_]| + |C_2[\_]| \leq 4$.

   The analysis is similar to the previous case.

□